有 趣 的 数 论

O.奥尔　著

潘承彪　译

有 趣 的 数 论

O. 奥尔 著

潘承彪 译

责任编辑 徐信之

*

北京大学出版社出版

(北京大学校内)

北京大学印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

787×1092毫米 32开本 4.25印张 88千字

1985年2月第一版 1985年2月第一次印刷

印数：00001—40,000册

统一书号：13209·102 定价：0.75元

致 读 者

这本书是专业数学家编写的一套丛书中的一本。编写这套书的目的是要向广大的中学生和非专学数学的外行人把一些重要的数学概念说明得有趣且能懂。“新数学丛书”中的大多数书所讨论的课题通常不属于中学课程表的范围。各书的难易程度不同，甚至在同一本书里，有些部分就比其它部分更需要全神贯注才能读懂。虽然读者要懂得这套丛书中的大多数书，并不需要多少专门知识，但是他必须动一番脑筋。

如果读者从来只在课堂上才遇到数学，那他就应该牢记：数学书不能读得很快，他也一定不要期望，读第一遍的时候就能理解书的全部内容。复杂的部分他应该自由地跳过去，以后再回过头来读；一个论点常常是通过后面的话才能搞清楚。另一方面，内容十分熟悉的一些节可以读得很快。

学数学的最好办法是“做数学”；每一本书都包含问题，其中有些可能需要很可观的思考。劝告读者养成读书时手边备有纸和笔这一习惯，这样读，他会越来越觉得数学有趣味。

这套书的编印是一种新的冒险。我们愿在此申明并致谢，在准备这套书时，许多位中学师生曾慷慨协助。编辑者欢迎读者提出意见．请函告 Editorial Committe of the NML series, New York University, The Courant Institute of Mathematical Sciences, 251 Mercer Street, New York, N.Y. 10012, [U.S.A.]。

编辑者

作 者 简 介

奥伊斯坦·奥尔(Oystein Ore) 1899 年出生于挪威奥斯陆。1922年奥斯陆大学毕业之后，他到德国哥丁根大学继续研究数学，随后成为瑞典 Mittag-Leffler 研究所成员，并于1924年在奥斯陆获得哲学博士学位。第二年他是作为国际教育委员会成员，在巴黎和哥丁根渡过的，后来他成为奥斯陆大学副研究员。1927年他接受了耶鲁大学的邀请，从此开始了他在美国的事业。从1931年起，他成为耶鲁大学斯脱林讲座教授(Sterling Professor)。

从1936年到1945年，奥尔教授是耶鲁大学数学系系主任。他除发表了许多数学论文外，还写了不少书，其中内容较为初等的书有：《数论及其历史》(Number Theory and its History,1948)；《卡达诺，赌博学家①》(Cardano, the Gambling Scholar, 1953)；以及《尼尔斯·亨利克·阿贝尔——数学的奇才》(Niels Henrik Abel, Mathematician Extraordinary, 1957)。后期，他对图论特别有兴趣，写的书有：《图及其应用》(Graphs and Their Uses, 1963)，这是本丛书的第十册；《图论》(Theory of Graphs, 1962)；《四色问题》(The Four-Color Problem, 1967)。

1968年8月13日奥尔教授不幸于奥斯陆逝世，并安葬在那里。

---

① G. Cardano (亦名J. Cardan, 1501—1576) 是欧洲文艺复兴时期的著名学者，通常把三次代数方程的求解公式称为 Cardano 公式。——译者

目　　录

第一章　引　言

§1.1　由来

数论是数学的一个分支，它研究自然数

1，2，3，…

的性质，自然数通常称为正整数。

考古学和历史告诉我们，人很早就会计数。先会做数①的相加，很久以后才会做数的相乘和相减。当为了要平均分配大量的苹果或捕获的鱼时，数的相除就是必要的了。这些数的运算统称为计算(calculations)。"calculation"一字起源于拉丁字calculus，是小石子的意思。古罗马人在他们的计算板上就是用小卵石来表示数的。

当人们一旦知道了一些如何对数进行计算后，它就成为一种有趣的智力游戏。多少世纪以来，从各种各样的兴趣积累起来了如此之多的有关数的经验知识，以至今日可以说，在现代数学中，我们有了被称为数论的这样一个使人赞赏不已的，既丰富又漂亮的，结构严谨的分支。它的某些部分仍是简单的数字游戏，而另一些则是数学中最困难、最复杂的问题。

§1.2　数的玄学②

我们确实可以在有关数的迷信中，发现一些最早期的关

① 本书前六章中的"数"，未加说明者，均指自然数及零。——译者

② 我们把"Numerology"译为"数的玄学"，亦可译为"命理学"。——译者

于数的思想的形迹，在每个民族中都能找到这种例子。有为人偏爱的幸运之数，也有被人视为灾难而避开的不祥之数。我们有许多关于古希腊的数的玄学的资料，这种数的玄学，是他们关于各种数的象征性意义的看法和迷信。例如，大于1的奇数象征男性，而偶数则表示女性。数5是第一个男性数与第一个女性数之和，因此它象征着结婚或联合。

要想进一步知道更多的关于数的玄学的例子的人，可以去图书馆借阅柏拉图(Plato)所著的《共和国》一书的第八册。而这种数的玄学，从数学观点来看，是没有多大意义的，因为数学所要研究的是数的运算及其性质。但正如我们即将看到的，某些仍为数学家所研究的著名数论问题确是出于希腊的数的玄学。

至于对数的迷信，现在已没有多大理由会使我们感到神秘了。然而，大家都知道，女主人们绝不愿意在其餐桌上有13位客人；极少的旅店有第13号房间或13层楼。我们实在不清楚为什么要忌讳这个数。虽有许多解释，但绝大多数是没有多少根据的。例如，我们都记得在《最后的晚餐》上有13位客人，而第13个当然就是犹大。

在圣经，特别在旧约中，数7起着特殊的作用；在古老的德国民间传说中，数3与数9经常重复出现；还有，信奉印度教的印度人，在其神话中特别偏爱数10。

§1.3 毕达哥拉斯问题

我们可以提出毕达哥拉斯(Pythagorean)问题来作为早期数论的一个例子。我们知道，在一个直角三角形中，边长满足毕达哥拉斯关系式：

$$z^2 = x^2 + y^2, \qquad (1.3.1)$$

其中 z 是斜边长。这一关系式使我们有可能在直角三角形中，当两边的长度已知时，去计算出第三边的长度。顺便说一下，以希腊哲学家毕达哥拉斯的名字来命名这一定理是有些不恰当的，因为差不多比他的时代要早两千年，巴比伦人就知道了这个定理。

有时，式（1.3.1）中的边长 x，y，z 都是整数。最简单的情形

$$x=3,\quad y=4,\quad z=5, \tag{1.3.2}$$

已经在巴比伦的泥版上发现了。我们可以把这一情形作如下的解释：假定有一根铁丝，我们在其上标上记号或者打结，将它分为十二等份。那末，当我们绕着固定在地上的三个小柱子拉紧铁丝，得到一个两边长度分别为 3 与 4 的三角形时，第三边的长度就为 5，并且其所对的角必为直角（图 1.3.1）。我们经常可以在数学史中读到，在尼罗河泛滥之后，当埃及的土地测量人员在丈量土地时，就是利用这一方法来作直角三角形的。然而，这很可能是科学史中很多虚构的故事之一，因为至今还没有找到这一说法的根据。

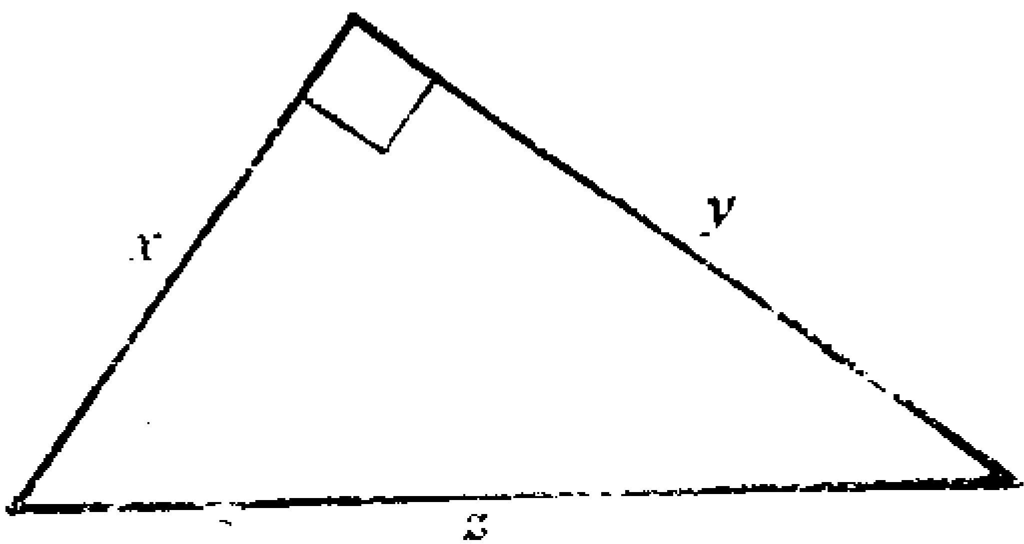


图 1.3.1

毕达哥拉斯方程(1.3.1)还有许多其它的整数解，例如，

$$x=5,\quad y=12,\quad z=13,$$

$$x=7,\quad y=24,\quad z=25,$$

$$x=8,\quad y=15,\quad z=17.$$

以后我们将指出，如何去求所有这样的解。希腊人知道如何去确定它们，有可能巴比伦人也知道。

当给定两个整数 x 和 y 后，总能找到一个相应的 z 满足式（1.3.1），但 z 很可能是无理数。当我们要求三个数全为整数时，它们所可能取的值就受到了严格的限制。亚历山大城的希腊数学家丢番图（Diophantos）（年代不详，约为公元200年左右）写了一本研究这类问题的书《算术》。从此，求方程的整数解或有理数解的问题就称为丢番图问题，而丢番图分析是现代数论的一个重要组成部分。

习　题

1. 试求几个毕达哥拉斯方程的其它的整数解。

2. 试再求出几个这样的整数解：使其斜边比较长的直角边长一个单位。

§1.4　形数

在数论中，我们经常碰到平方数，如

$$3^2=9,\quad 7^2=49,\quad 10^2=100,$$

以及立方数，如

$$2^3=8,\quad 3^3=27,\quad 5^3=125.$$

这种数的几何表示方法是我们从希腊数学思想中继承下来的许多遗产之一。希腊人喜欢把包括整数在内的所有的数都看作为几何量。因此，乘积 $c=a\cdot b$ 就被看作是边长为 a 与 b 的矩形的面积。我们也可以把 $a\cdot b$ 看作是一边有 a 个点，另一边有 b 个点的矩形点阵中的点的个数。例如，$20=4\cdot5$ 就是图1.4.1的矩形点阵中的点的个数。

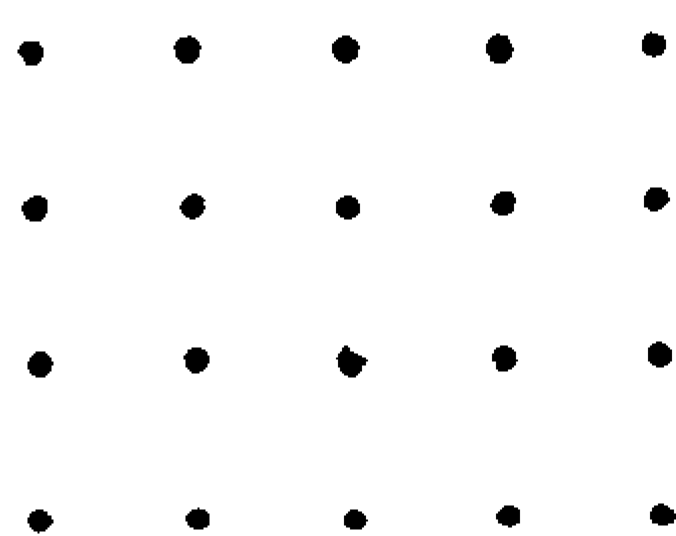


图　1.4.1

任何一个整数，如果它是两个整数的乘积，就可称为**矩形数**。当这矩形的两边有同样的长度时，这个数就是平方数。某些数除了用排列在一行上的点这种显然的方式来表示外，不能表为其它形状的矩形数。例如，5仅能表为一边是1个点，而另一边是5个点的矩形数（图1.4.2）。希腊人称这种数为**素数**。他们通常不把单独的一个点看作为数。单位1是用以构造出所有真正的数的“基砖”。这样，**1过去不是，现在也不是素数。**

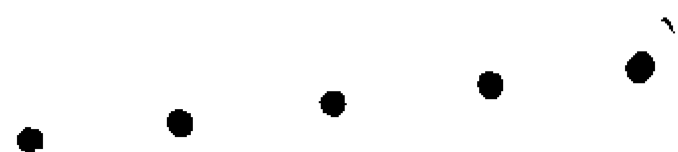


图 1.4.2

代替矩形和正方形，我们可以考虑规则地位于其它几何图形中的点。在图1.4.3中，画出了开头几个相邻的**三角数**。

一般地，第n个三角数由公式

$$T_n = \frac{1}{2}n(n+1), \quad n=1,2,3,\cdots \qquad (1.4.1)$$

给出。这些数有许多性质。例如，两个相邻的三角数之和是一个平方数：

$$1+3=4, \quad 3+6=9, \quad 6+10=16 \qquad (1.4.2)$$

等等。

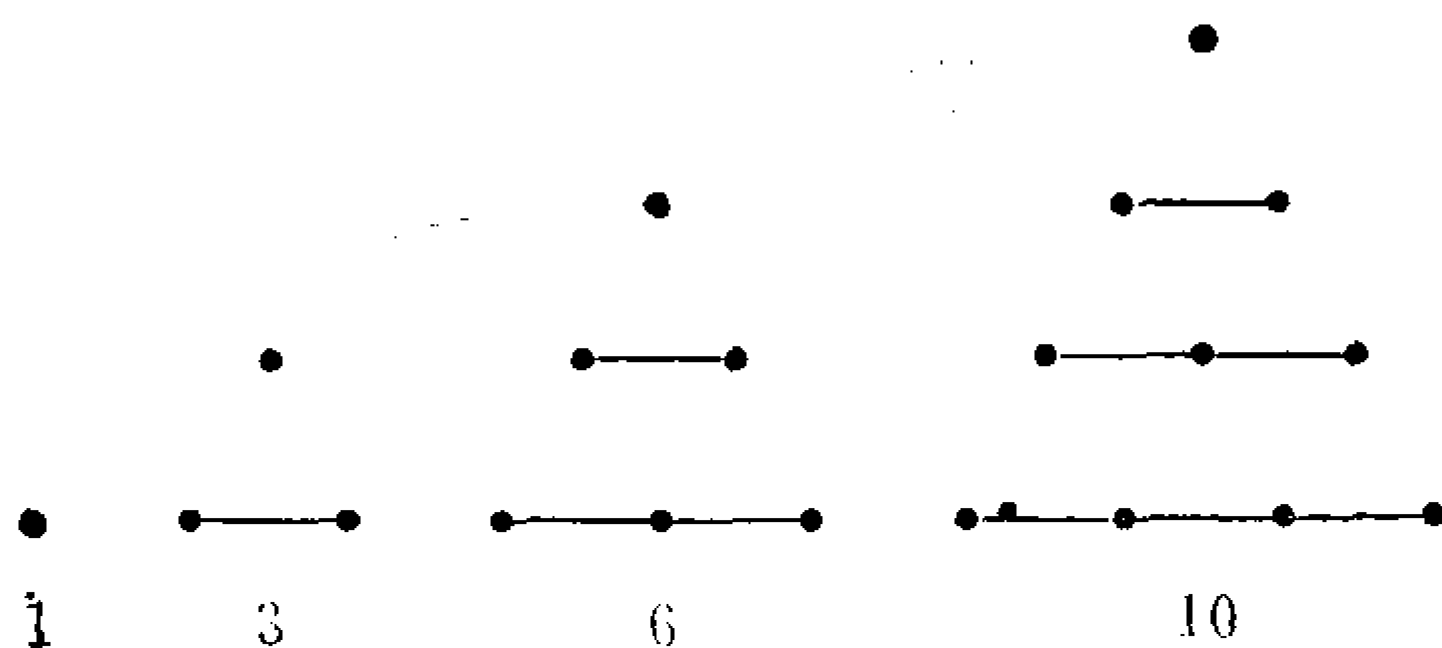


图 1.4.3

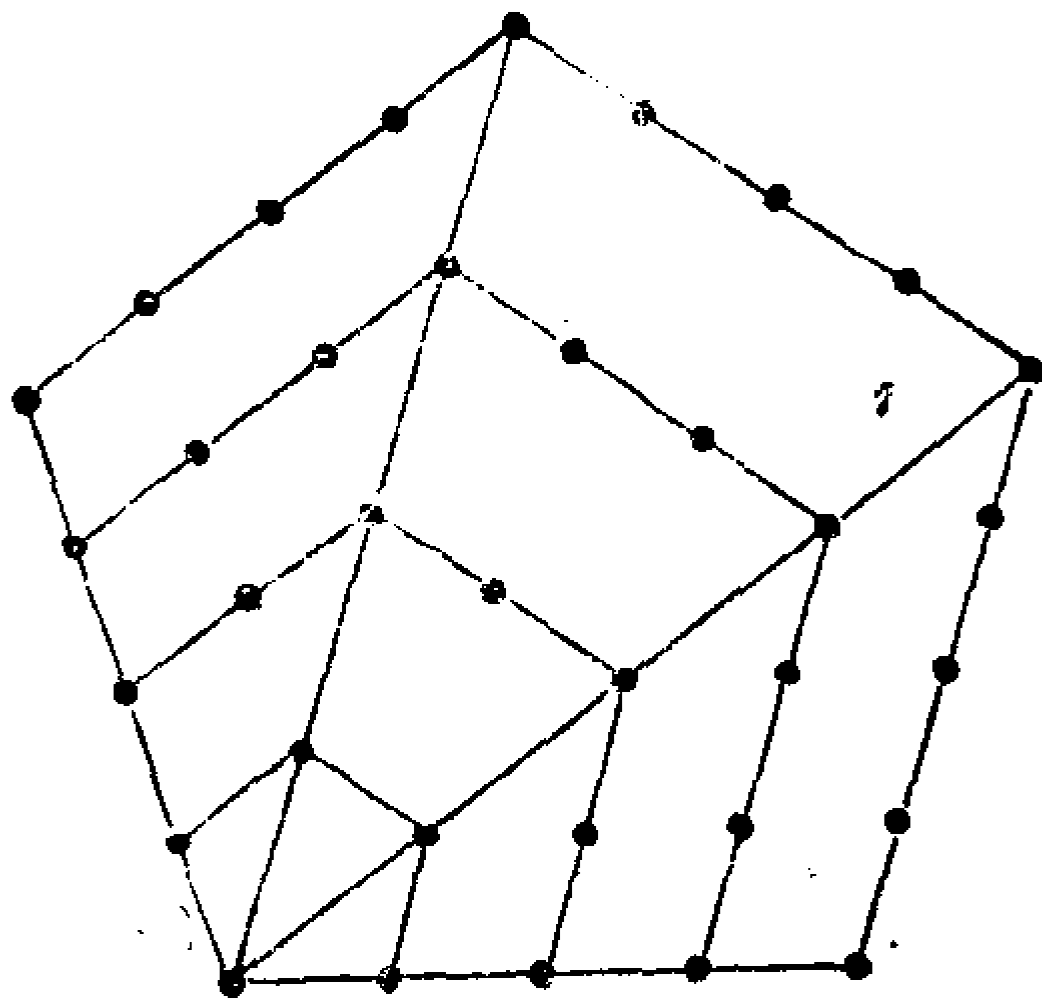


图 1.4.4

三角数与平方数已被推广为更一般的多角数。让我们用图1.4.4所定义的五角数来说明这一点。

可以看出，开头几个五角数是

$$1,\ 5,\ 12,\ 22,\ 35. \tag{1.4.3}$$

可以证明第 n 个五角数 p_n 由公式

$$p_n = \frac{1}{2}(3n^2 - n) \tag{1.4.4}$$

给出。类似地，可以得到六角数，以及一般地由正 k 边形来定义的 k 角数。我们不再花费时间来讨论它们了。希腊的数论传入西欧之后，形数，特别是三角数，在文艺复兴后期的数的研究中是十分普遍的。偶尔，它们还在现代的数论文章中出现。

从这种几何分析中，可以推出一些简单的数的关系式。我们仅来指出一个事实。人们很早就发现了：当把奇数相加到某一个数为止时，所得的结果总是一个平方数，例如

$$1+3=4,\quad 1+3+5=9,$$
$$1+3+5+7=16,$$

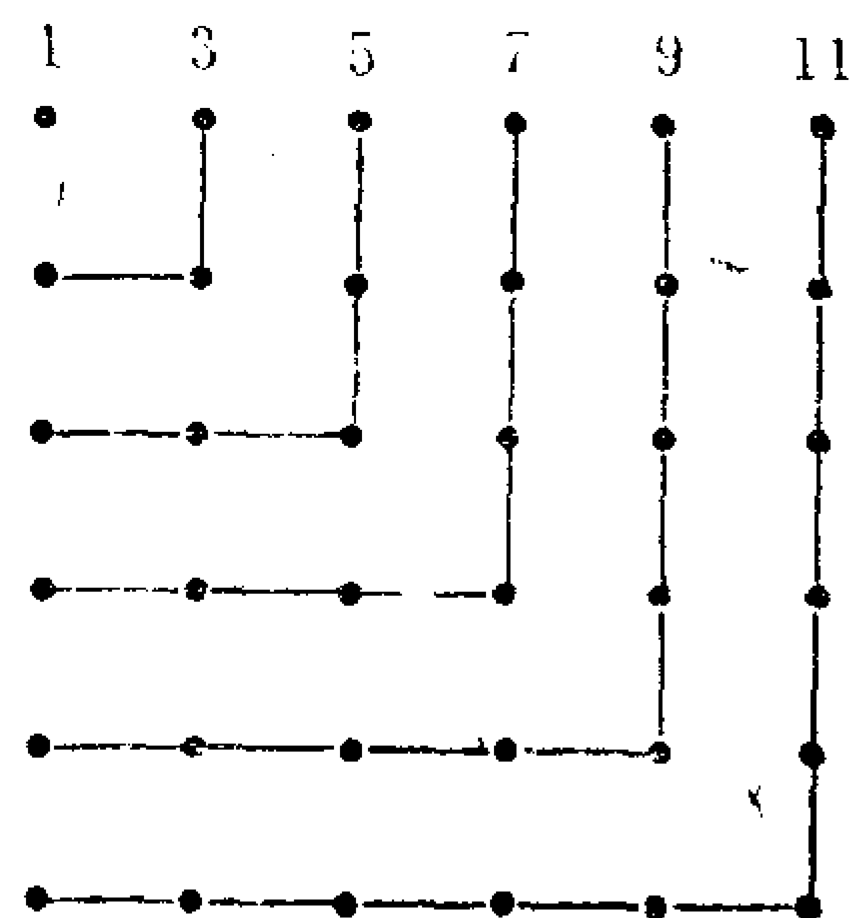


图 1.4.5

等等。为了证明这个关系式，我们只要看一下图1.4.5中画的一串重叠的正方形就清楚了。

习　题

1. 用归纳法证明三角数的通项公式（1.4.1）。
2. 证明五角数的公式（1.4.4）。
3. 证明k角数的通项公式是

$$\frac{1}{2}k(n^2-n)-n^2+2n.$$

§1.5　幻方

如果你曾玩过一种游戏板的话，你应记得在板上有九个方格，上面有编号1到9按图1.5.1的样式排列。

游戏者力争把小圆片投放于编了号的方格中。这里，将每一行，每一列，以及每一条对角线上的数字加起来有同样的总和——15。

一般说来，一个**幻方**是指1到n^2，这n^2个整数的这样一种正方形排列：使其每一行，每一列，及每一条对角线上的数字相加都有同样的和s，s称为**幻和**。图1.5.2给出了$4^2=16$个数组成的一个幻方。这里幻和等于34。

对每一个n仅有一个幻和s，且很容易求出其值。因为每一行的和为s，共有n行，所以幻方中所有的数之和为ns。但另一方面，由算术级数的求和公式知，从1到n^2的所有的数之和是

$$1+2+\cdots+n^2=\frac{1}{2}(n^2+1)n^2.$$

2	9	4
7	5	3
6	1	8

图 1.5.1

1	8	15	10
12	13	6	3
14	11	4	5
7	2	9	16

图 1.5.2

因此，

$$ns = \frac{1}{2}(n^2 + 1)n^2.$$

由此推得

$$s = \frac{1}{2}n(n^2 + 1). \qquad (1.5.1)$$

所以若 n 给定，那末 s 就确定了。对所有大于 2 的 n 都可以作出幻方；但读者容易验证，当 $n = 2$ 时，这样的幻方是不存在的。

在中世纪，这些正方形的这种不可思议的性质被认为是有奇异的魔力，因而它们被用来作为护身符，以保护佩戴者免受祸害．在 A．度勒(Albrecht Dürer，1471—1528)的著名版画《忧郁症》(Melancholia) 中的幻方是经常被复制的一个(见图1.5.3)。顺便指出，这个幻方也告诉了我们，当时这些数字度勒是如何写出来的。最后一行中间的两个数代表1514年，我们知道度勒的版画正是作于这一年。他可能正是从这两个数出发，通过不断的试验而找出了其余的数字。

图 1.5.3

我们可以证明：当$n=3$时，本质上只有一个幻方，即图1.5.1中的那一个。为此，我们先写出一个一般形式的表

$$\begin{matrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{matrix}$$

并来考察这九个数可能取什么值。

首先，我们指出中心的数 y_2 一定是 5。为此，我们注意到，由式（1.5.1）知，当$n=3$时，其幻和 $s=15$。我们分别把在第二行，第二列及二条对角线上的三个数加起来，可以看出，除 y_2 外，每一个数都在这些和中只出现一次，而

y_2 出现了四次，因为它在这四个和的每一个中均出现。又因为每一个和都等于 s，所以我们有

$$
\begin{aligned}
4s &= 4\times 15 = 60 \\
&= x_2+y_2+z_2+y_1+y_2+y_3+x_1+y_2+z_3 \\
&\quad +z_1+y_2+x_3 \\
&= 3y_2+x_1+x_2+x_3+y_1+y_2+y_3+z_1+z_2+z_3 \\
&= 3y_2+1+2+\cdots+9 \\
&= 3y_2+45.
\end{aligned}
$$

因此，

$$3y_2=60-45=15, \quad 即\ y_2=5.$$

在

$$
\begin{matrix}
x_1 & y_1 & z_1 \\
x_2 & 5 & z_2 \\
x_3 & y_3 & z_3
\end{matrix}
$$

这个格式中，数 9 不能出现在角上。因为，比如若 $x_1=9$，那末 $z_3=1$（因 $s=15$），而这正方形将是

$$
\begin{matrix}
9 & y_1 & z_1 \\
x_2 & 5 & z_2 \\
x_3 & y_3 & 1
\end{matrix}
$$

因为 $y_1+z_1=x_2+x_3=6$，所以这四个数 y_1,z_1,x_2,x_3 一定都小于 6，而我们仅剩下了三个小于 6 的数，即 2，3 及 4，因此这是不可能的。这就证明了 9 一定位于一行或一列的中间，所以我们的正方形可取为

$$
\begin{matrix}
x_1 & 9 & z_1 \\
x_2 & 5 & z_2 \\
x_3 & 1 & z_3
\end{matrix}
$$

数 7 不能与 9 位于同一行，因为它们的和超过15；数 7 也不能与 1 位于同一行，因为这时那一行上剩下的数也应是 7 。故 7 不能位于角上，并可假定这正方形有如下的格式：

$$
\begin{matrix}
x_1 & 9 & z_1 \\
7 & 5 & 3 \\
x_3 & 1 & z_3
\end{matrix}
$$

这样， 9 所在的那一行中的其它两个数必是 2 与 4 ，因为不然的话，其和将超过15。进而， 2 必定与 7 在同一列，因为若 4 在那里的话，这一列的第三个数也将为 4 。通过这样的考察可以确定剩下的两个数 6 与 8 的位置，这样，我们就得到了图1.5.1中所示的幻方。

对于较大的 n 可以作出很多不同的幻方。有如今日的纵横字谜游戏一样，在十六、十七世纪，甚至还更晚，构造幻方非常盛行。本杰明·弗兰克林 (**Benjamin Franklin**) 是一个幻方迷。后来，他承认：当他任宾夕法尼亚州议会的职员时，为了消磨那乏味的办公时间，他填出了一些特殊的幻方，甚至一些幻圆——它是这样构成的，在一些按一定规则分布的互相相交的圆的交点处，填上一定的数字，使得每个圆上的数字之和相等。以下的内容取自《本杰明·弗兰克林文集》第四卷，第392—403页(耶鲁大学出版社)。

弗兰克林的幻方为人所知并显其异采，有这样一段有趣的经过。弗兰克林有一个朋友叫洛根(Logan)，一天他给弗兰克林看几本关于幻方的书，并说道：他不相信任何一个英国人，曾经做出过任何这类出色的事情来。“然后，他在这本书中指给我看了几个不常见的、较为奇妙的幻方。但当我认为它们中，沒有一个同我记得我曾作的一些幻方一样时，

他要求看看这些幻方。于是，下一次我去拜访他时，就带了一个在我的旧文件中找到的 8 阶（$n=8$）幻方给他。现在我给你们看看这个幻方，并说明它的性质。”（图1.5.4）。

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

图 1.5.4

弗兰克林仅对他的幻方提出了几个性质，我们让读者自己去发现更多的性质。我们看到幻和 $s=260$，而且将每半行，每半列加起来等于130，即260的一半。角上的四个数与中间的四个数之和为 260。从16到10，再从 23到17所组成的“折线”上的数字之和也为 260。同样的，与此平行的每一个“折线”上的 8 个数之和也为260。

“然后，洛根先生给我看一本古老的四开本的算术书①，我记得是一个叫史坦非留斯的人写的。这本书中有一个16阶幻方。他说：想来这一定是一项花费了巨大劳动的工作。但是，如果我没有忘记的话，这个幻方只具有最普通的性质：分别将每一个水平的，垂直的以及对角线上的数字相加都具有相同的和，即2056。”

① 这本书是 Michael Stiefel 所著的 Arithmetica integra, Nürnberg, 1544.

“我不愿意在构造幻方上，让史坦非留斯先生胜过我，即使仅仅在幻方的大小上。当晚我回家后，就作出了下面的这个16阶幻方。它除了具有前面的那个 8 阶幻方所有的全部

A Magic Square of Squares.

200	217	232	249	8	25	40	57	72	89	104	121	136	153	168	185
58	39	26	7	250	231	218	199	186	167	154	135	122	103	90	71
198	219	230	251	6	27	38	59	70	91	102	123	134	155	166	187
60	37	28	5	252	229	220	197	188	165	156	133	124	101	92	69
201	216	233	248	9	24	41	56	73	88	105	120	137	152	169	184
55	42	23	10	247	234	215	202	183	170	151	138	119	106	87	74
203	214	235	246	11	22	43	54	75	86	107	118	139	150	171	182
53	44	21	12	245	236	213	204	181	172	149	140	117	108	85	76
205	212	237	244	13	20	45	52	77	84	109	116	141	148	173	180
51	46	19	14	243	238	211	206	179	174	147	142	115	110	83	78
207	210	239	242	15	18	47	50	79	82	111	114	143	146	175	178
49	48	17	16	241	240	209	208	177	176	145	144	113	112	81	80
196	221	228	253	4	29	36	61	68	93	100	125	132	157	164	189
62	35	30	3	254	227	222	195	190	163	158	131	126	99	94	67
194	223	226	255	2	31	34	63	66	95	98	127	130	159	162	191
64	33	32	1	256	225	224	193	192	161	160	129	128	97	96	65

B. Franklin inv. J. Ferguson delin. J. Mynde sc.

图 1.5.6

性质外，还有这样的性质：在一张纸上挖去这样大小的一个正方形孔，使其放在这个较大的正方形上时，恰好露出16个小正方形。那末不管我们把这张纸如何放在这个较大的正方形上，从这个孔中出现的16个数之和必为2056。”

这里是弗兰克林的幻方，你自己可以试一试去发现它的惊人的性质(图1.5.5)。

正如我们从他的信的结尾中可以看到的，弗兰克林有理由为他的创造感到骄傲。“第二天我把它送给我们的朋友。几天之后，他把这个幻方寄回，并在信中这样写道：‘今寄还您这一令人惊异不止的或最伟大的幻方，在这一幻方中…’但赞扬的话是太过份了，为了他，也为了我自己，我不应当在这里重复它。其实，这也是不必要的，因为我无疑地相信，你将会毫不犹豫地同意，这一16阶幻方是所有的幻方制作者所做出的幻方中，最神奇的一个。”

关于构造幻方的更多的知识，可看J. V. Uspensky和M. A. Heaslet合著的《初等数论》(Elementary Number Theory, 1939)。

习　题

1. 当度勒做他的幻方(图1.5.3)时，他能否用其它的幻方以同样的方式来标出这一年份？

2. 度勒一直活到1528年。他能否以同样的方式，在他后来的任一幅画中标出作画的年代？

3. 试指出弗兰克林幻圆(图1.5.6[①])的性质。

---

① 这是弗兰克林幻圆的复制品，彩色的原作最近在纽约的一次拍卖中被一个私人收藏家买去了。

A Magic Circle of Circles.

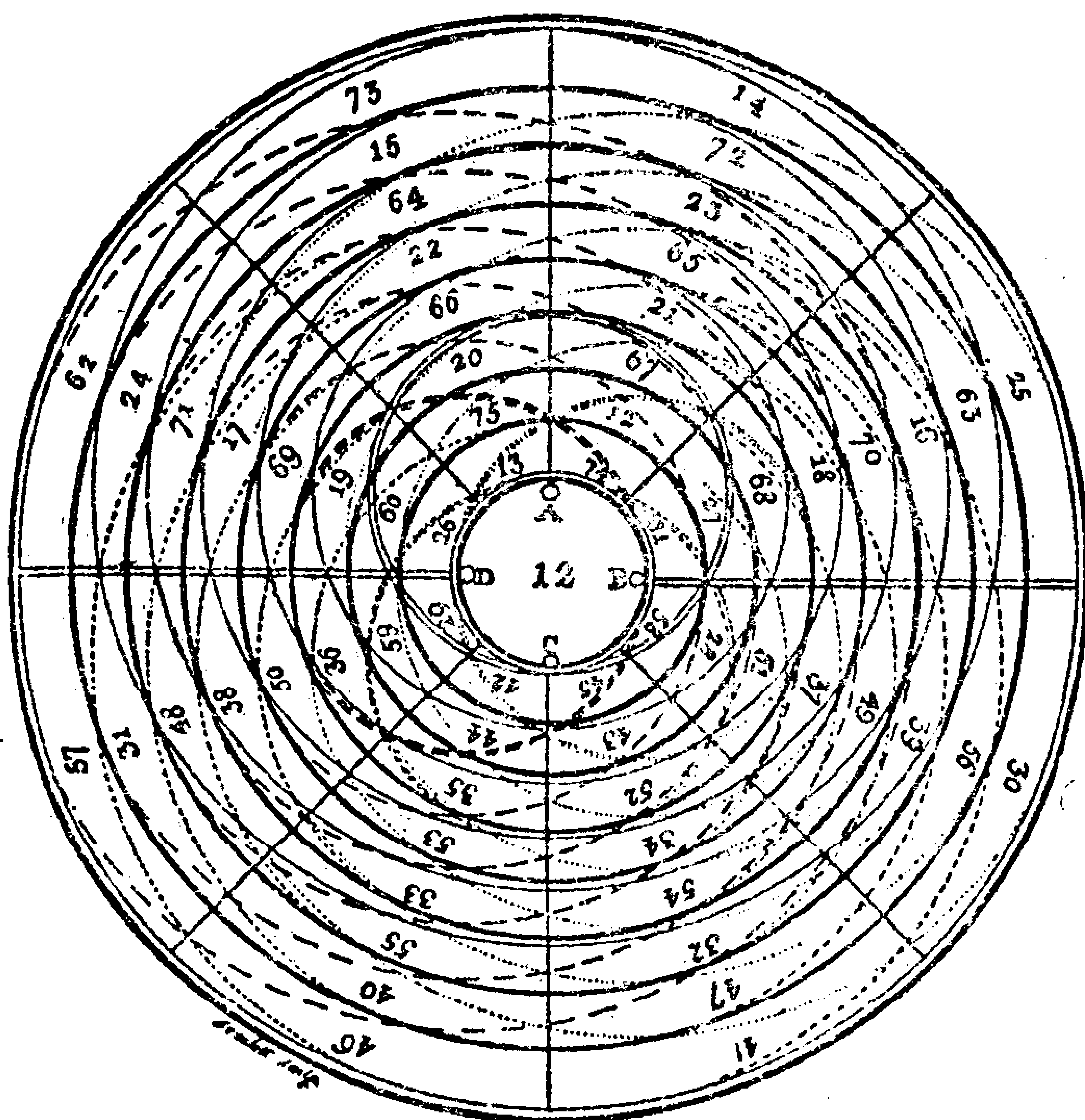


图 1.6.6

第二章 素　　数

§2.1 素数与合数

我们所发现的最重要的性质之一是：一些数能分解为两个或多个较小的因数的乘积，例如，

$$6=2\cdot3,\ 9=3\cdot3,\ 30=2\cdot15=3\cdot10,$$

而另一些则不能，如

$$3,\ 7,\ 13,\ 37.$$

我们记得，一般当

$$c=a\cdot b \qquad (2.1.1)$$

是两个数 a 与 b 的乘积时，a 与 b 就称为是 c 的因数或除数。每一个数都有**显然分解**

$$c=1\cdot c=c\cdot1. \qquad (2.1.2)$$

相应地，我们称 1 与 c 为 c 的**显然除数**。

任意一个数 $c>1$，如果有非显然分解，就称为**合数**。当 c 仅有显然分解(2.1.2)时，就称为**素数**。在开始100个数中有以下25个素数：

2，3，5，7，11，13，17，19，23，29，31，37，41，
43，47，53，59，61，67，71，73，79，83，89，97；

除 1 以外，其余的数均是合数。我们来证明：

定理2.1.1 **任一整数 $c>1$，要么是一个素数，要么有一个素因数。**

证 若 c 不是素数，则它必有一个最小的非显然因数 p。该 p 必为素数。因为若 p 是合数，那末 c 就将有一个更小的因数。

这样，我们就提出了数论中第一个重要的问题：怎样来判定一个数是否是素数，以及当它是合数的情形时，怎样能求得一个非显然除数。

一个直接的，但极不令人满意的回答是：我们可以用所有比给定的数 c 小的数去试除它。根据定理 2.1.1，只要用所有的比 c 小的素数去除就可以了。注意到下面的事实，我们就能大大地减少这一繁重的工作：在分解式(2.1.1) 中，因数 a 和 b 不可能同时大于$\sqrt{c}$。因为，如果这样，则有

$$a \cdot b > \sqrt{c} \cdot \sqrt{c} = c,$$

而这是不可能的。因此，为了知道 c 是否有一个非显然除数，我们只需要验证是否有小于或等于$\sqrt{c}$ 的素数能整除 c。

例 1 若 $c=91$，则$\sqrt{c}=9.\cdots$。以素数 2,3,5,7 试除后，可看出$91=7\cdot 13$。

例 2 若 $c=1973$，可求得$\sqrt{c}=44.\cdots$。因为所有不超过43的素数都不能整除 c，所以这个数是素数。

我们马上就会看出，这一方法对于大数可以是十分麻烦的。然而，和许多其它的数论计算一样，这里可以利用现代技术。给计算机编一个这样的程序是很简单的：用所有不超过$\sqrt{c}$的整数去除 c，并打印出那些没有余数，即整除 c 的那些数。

另一个十分简单的方法是求助于素数表，即利用已由其它方法得到的素数来进行检查。在前两个世纪中，编造和出版了许多素数表。最大、最实用的表是 D.N.雷麦(Lehmer)编制的，给出了10,000,000以内的全部素数①。我们的表 1

① D.查基尔(Zagier)最近编制了不超过50,000,000的素数表．——译者

包含了1000以内的全部素数。

某些热心的计算者确实已经编制了一些超过10,000,000的素数表。然而，花费巨大的代价去出版这样的表，看来是没有多大用处的。很少有一个数学家，甚至一个数论专家，会碰到要去判定一个很大的数是否是素数这样的问题。此外，一个数学家并不是任意抓住一个大数就去判定它是合数还是素数，他所要判定的数，通常总是出现在一些特殊的数学问题中，因而有非常特殊的形式。

表 1　1000以内的素数

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,

101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,

211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293,

307,311,313,317,331,337,347,349,353,359,367,373,379,383,389,397,

401,409,419,421,431,433,439,443,449,457,461,463,467,479,487,491,499,

503,509,521,523,541,547,557,563,569,571,577,587,593,599,

601,607,613,617,619,631,641,643,647,653,659,661,673,677,683,691,

701,709,719,727,733,739,743,751,757,761,769,773,787,797,

809,811,821,823,827,829,839,853,857,859,863,877,881,883,887,

907,911,919,929,937,941,947,953,967,971,977,983,991,997.

习　题

1. 下面的数中哪些是素数？

(a) 你出生的年份；

(b) 今年的年份数；

(c) 你家的门牌号。

2. 求出大于素数1973的下一个素数。

3. 注意到从90到96(包括90和96在内)是七个相邻的合数，试再求出 9 个相邻的合数。

§2.2 麦生素数

素数竞赛已经进行了好几个世纪。许多数学家都在争夺发现最大素数的荣誉。当然可以选择一些不具有 2,3,5,7 这样显而易见的除数的很大的数，然后去考查它们是否为素数。正如我们即将看到的，这不是一个很有效的方法，而现在这场竞赛已经固定地沿着一条被证明是成功的，单一的途径来进行了。

麦生素数是指具有特殊形式

$$M_p = 2^p - 1 \qquad (2.2.1)$$

的素数，其中 p 为另一素数。这种数早就出现于数学之中，在欧几里得(Euclid) 关于完全数（我们将在下面看到）的讨论中就出现了。这些数是以法国修道士 M. 麦生(Marin Mersenne，1588—1648)的名字命名的，这是因为他作了大量的关于完全数的计算。

当我们开始对不同的素数 p 计算形如式(2.2.1)的数时，就将发现它们并非全为素数。例如，

$$M_2 = 2^2 - 1 = 3 = \text{素数},$$
$$M_3 = 2^3 - 1 = 7 = \text{素数},$$
$$M_5 = 2^5 - 1 = 31 = \text{素数},$$
$$M_7 = 2^7 - 1 = 127 = \text{素数},$$

$$M_{11}=2^{11}-1=2047=23\cdot 89.$$

寻求大的麦生型素数的一般方法，是对各个素数 p 去判明所有的数M_p。这种数增长得十分迅速，所以，所需要的计算量也迅速增加。然而，这一工作甚至对于十分大的数也是容易完成的，其原因是，有一些十分有效的方法，可用来断定这些特殊的数是否为素数。

到1750年瑞士数学家欧拉(Euler)证明M_{31}是素数为止，是寻找麦生素数的初级阶段。到那时已经发现了八个麦生素数，它们对应于

$$p=2,\quad p=3,\quad p=5,\quad p=7,$$
$$p=13,\quad p=17,\quad p=19,\quad p=31.$$

欧拉的数M_{31}在一个多世纪中，一直是已知的最大素数。1876年法国数学家罗卡斯(Lucas)证明了一个巨大的数

$M_{127}=170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727$

是素数。这是多么大的一个数，它有39位数字！小于它的所有麦生素数是由上面的那些 p 值，再加上

$$p=61,\quad p=89,\quad p=107$$

给出。这 12 个麦生素数完全是靠笔和纸计算得到的(对后面的几个利用了机械台式计算机)。由于电动计算机的应用，使得有可能继续研究到 $p=257$，但结果是令人失望的，没有新的麦生素数被发现。

应用电子计算机后的情况是这样的：随着大容量机器的发展，使我们有可能在愈来愈大的限度内来研究麦生素数。D.H.雷麦(Lehmer)证明了

$$p=521,\quad p=607,\quad p=1279,$$
$$p=2203,\quad p=2281$$

给出麦生素数 M_p。随后，又有一些进展。黎塞尔(Riesel,

1958)指出

$$p = 3217$$

给出一个麦生素数，而赫尔维茨(Hurwitz,1962)又发现了另外两个值

$$p = 4253, \qquad p = 4423.$$

吉里斯 (Gillies,1964) 作出了巨大的推进，他发现了相应于

$$p = 9689, \quad p = 9941, \quad p = 11213$$

的麦生素数。

以上给出了至今人们所得到的全部23个麦生素数①，我们可以期望随着机器容量的增加，而发现更大的麦生素数。正如我们所指出的，罗卡斯的素数有39位数字。即使只是去计算出最大的已知素数 M_{11213}也是一件相当繁重的工作，而且看来也沒有必要在这里把它给出来。但是，我们可能有兴趣想知道它有多少位数字。这就用 不 着 眞 正地去计算这个数，而可以按下面的方法来做。

代替 $M_p = 2^p - 1$ 我们来求它的下一个数

$$M_p + 1 = 2^p$$

的位数。这两个数一定有相同的位数。因为，假如$M_p + 1$要多一位数，那末它的末位数必为 0 ，但这对 2 的任意次幂是不可能的。因为从数列

$$2, \ 4, \ 8, \ 16, \ 32, \ 64, \ 128, \ 256, \cdots$$

可以看出，它们的末位数只可能是数2,4,6,8中的一个。

我们利用 $\log 2^p = p \cdot \log 2$ 来求 2^p 的位数。从表可得log2的近似值为0.30103，所以

---

① 到1979年为止，发现了 27 个麦生素数，新发现的四个所对应的值是：$p = 19937, 21701, 23209, 44497$，而且在 $p < 50000$ 中，没有其它麦生素数．1983年又发现 $p = 86243$ 时也给出一个麦生素数．——译者

$$\log 2^p = p \cdot \log 2 = p \cdot 0.30103.$$

在 $p=11213$ 的情形下，给出

$$\log 2^{11213} = 3375.449\cdots,$$

因而，由 3375 我们得知，数 2^p 有3376位数字。所以我们能够说：目前所知道的最大素数有 3376 位数字(这里“目前”两字是本质的①)。这是在伊利诺大学的计算机上算出来的。该校的数学系为它所取得的这一成就而感到骄傲，为让全世界都羡慕它的成就，在它寄出的每一封信上都印上了这个数。

§2.3 费马素数

还有另外一种有很长而有趣的历史的素数：费马素数。这些数最初是由一个法国的法官费马(Fermat，1601—1665)所引进的。他业余爱好数学，是位杰出的数学家。最初的五个费马素数是

$$F_0 = 2^{2^0}+1=3, \quad F_1 = 2^{2^1}+1=5, \quad F_2 = 2^{2^2}+1=17,$$

$$F_3 = 2^{2^3}+1=257, \quad F_4 = 2^{2^4}+1=65537.$$

根据这一列数可以看出，费马素数的一般公式应该是

$$F_n = 2^{2^n}+1. \tag{2.3.1}$$

虽然，除了上面所给出的五个数外，费马没有作进一步的计算，但他坚信所有的这种数都是素数。然而，当瑞士数学家欧拉再往前走了一步，这个猜想就被推翻了。他证明了下一个费马数

$$F_5 = 4294967297 = 641 \cdot 6700417$$

不是素数。这个故事并没有因此结束，费马数后来又出现在

① 目前知道的最大的麦生素数为 $p=86243$，它有25962位.——译者

用直尺和圆规来作正多边形这样一个完全不同的问题中。

正多边形是这样一种多边形：它的顶点等距离地位于一个圆周上（图2.3.1）。如果它有 n 个顶点就称为**正 n 边形**。从顶点到圆心的 n 条联线构成了 n 个中心角，每一个角为

$$\frac{1}{n}\cdot 360^{\circ}.$$

如果能够画出这样大小的一个角，那末也就能够画出这个正 n 边形。

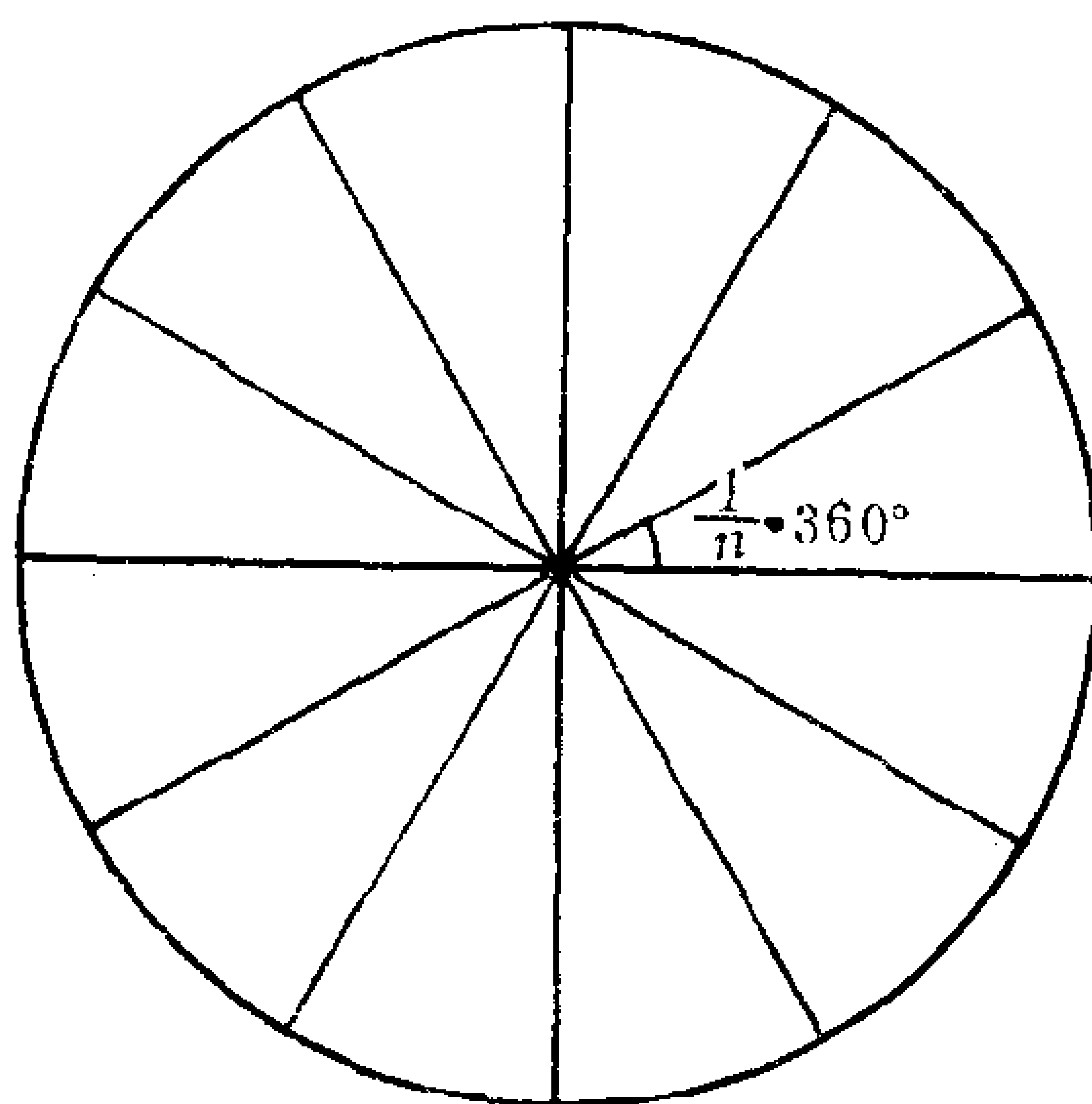


图 2.3.1

古希腊人对于寻找用圆规和直尺作正多边形的方法十分感兴趣。当然，对于等边三角形和正方形，这些最简单的情形，他们是会作的。利用不断地平分中心角的方法，他们能够作出具有

$$4,\ 8,\ 16,\ 32,\ \cdots,$$
$$3,\ 6,\ 12,\ 24,\ \cdots$$

个顶点的正多边形。此外，他们还能作正五边形，因此，也能作出具有

$$5,\ 10,\ 20,\ 40,\ \cdots$$

个顶点的正多边形。这样一来，又可以得到另外一种正多边形，正十五边形的中心角是

$$\frac{1}{15}\cdot 360^{\circ}=24^{\circ},$$

而这可由正五边形的中心角72°及正三边形的中心角 120° 来作出：第一个角的两倍减去第二个角。因此，我们能够作出边数为15,30,60,120,…的正多边形。

直到年轻的德国数学家 C.F. 高斯 (Gauss,1777—1855) 1801年发表了数论的划时代的著作《算术研究》(Disquisitiones Arithmeticae)，这个问题才有新的进展。高斯超过希腊几何学家的，不仅仅是他给出了一个利用圆规和直尺来作正十七边形的方法，更重要的是对所有的 n，他解决了哪些正 n 边形可以这样作出来，而哪些则不能。下面我们来叙述高斯的结果。

上面已经指出，从一个正 n 边形出发，通过等分它的每一个中心角，就能得到正$2n$边形。而另一方面，从一个正$2n$边形出发，只要简单地取其不相邻的 n 个顶点就能得到正 n 边形。这表明为了判定哪些正多边形可以作出，只要讨论奇数的情形就足够了。高斯证明了：**一个具有 n 个顶点的正多边形，当且仅当 n 是一个费马素数或是若干个不同的费马素数的乘积时，才能用圆规和直尺作出来。**

让我们来考察几个最小的值 n。可以看出，能够作出正三边形和正五边形，但不能作出正七边形，因为 7 不是费马素数。也不能作出正九边形，因为$9=3\cdot3$是两个相等的费马素数的乘积。也不能作出$n=11$或$n=13$的正多边形，但能够作出$n=15=3\cdot5$及$n=17$的正多边形。

很自然，高斯的发现引起了人们对费马数 (2.3.1) 的新的兴趣。在前一个世纪，为了寻求新的费马素数，沒有借助于机器进行了许多惊人的计算。现在利用电子计算机，以更快的速度正在继续进行这些计算。至今，所得到的结果是否定的，沒有新的费马素数被发现，因而，现在许多数学家倾

向于相信不再有其它的费马素数了。

习　题

1. 求出小于 100 的所有奇数 n，使得相应的正 n 边形可以被作出来。

2. 假定你已经会作正17边形，你如何来作正51边形？

3. 如果除了已经指出的五个费马素数外，不再有其它的费马素数了，那末可以作出多少个正 n 边形（n 为奇数）？最大的这种奇数 n 是多少？

§2.4　厄拉多塞筛法

正如已经说过的，我们有直到相当大的数为止的一些素数表。这样的表实际上是怎样来编造的呢？这个问题早已由亚历山大城的数学家厄拉多塞 (Eratosthenes，约公元前 200 年）所提出的一个方法解决了。他的办法是这样的：写出从 1 到任意一个我们所希望达到的数为止的全部整数：

1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	$\underline{9}$	$\underline{10}$	11	$\underline{12}$	13	$\underline{14}$	$\underline{15}$
			2		2		2	3	2		2		2	3.

由素数 2 开始。第一步是在 2 以后(但不包括 2 本身)的每两个数中的第二个数，即偶数 4，6，8，10 等的下面画上一短划来表示把它们都除去。做完这一步以后，第一个下面未加短划的数是 3。因为它不能被 2 整除，所以是素数。我们留下 3 不在其下面画上短划，但对 3 以后（不包括 3）的每三个数中的第三个数，即 6，9，12，15，…的下面画上短划；它们中的有一些因为是偶数，所以已经被画上过短划。在第二步中，第一个未画短划的是 5，它不能被 2 或 3 整除，所以

是素数。留下 5 不画短划。对 5 以后(不包括 5)的每五个数中的第五个数，即10,15,20,25,…中那些未被画上短划的数再画上短划。在这一步中，未画短划的最小的数是 7 ，它不能被任一较小的素数 2 ，3 ，5 所整除，所以是素数。重复这一步骤，直到最后得到一个由未被画上短划的数所组成的序列而结束。这些数，除了 1 以外，就是不超过我们所给定的数的全部素数。

这一筛选数的方法称为**厄拉多塞筛法**。所有的素数表都是根据这个筛法原则来编制的。事实上，利用计算机的储存能力，我们可以编制更大的素数表；利用这一手段，在洛斯·阿拉莫斯(Los Alamos)科学实验室中已经储存了不超过100,000,000的全部素数。

对以上的筛法稍作改变，就能得到更多的信息。假若每当这个数列中的一个数，第一次被画上短划时，就在这短划下面写出使这个数被除去的那个素数。例如，15和35：

$$\frac{15}{3}\ ,\quad \frac{35}{5}$$

以及在上面的数列中所标出的那些等等。这样一来，我们不但已经指出了素数，而且对每一个合数给出了整除它的最小素因数。这样的表称为**因数表**。因数表比素数表更加精细复杂。为了把因数表稍加简化，通常在表中不列出那些具有小素因数(如 2 ，3 ，5 ，7 等)的合数。现有的最大的因数表是D.N.雷麦编制的，包含直到10,000,000的全部整数。

正如我们已看到的，厄拉多塞筛法可用以编制素数表和因数表；而且它也能用于理论研究，近代数论的许多重要结果就是利用筛法证明的。最后，让我们来指出一个当时欧几里得所知道的事实：

素数有无穷多个.

证　假设只有 k 个素数

$$2, 3, 5, \cdots, p_k.$$

那末，在筛法中，p_k以后就将没有不画短划的数了. 但这是不可能的. 因为这些素数的乘积

$$P = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_k,$$

对每一个素数都被除去一次，共除去 k 次，所以它的下一个数$P+1$就不可能由于这些素数中的任何一个而被画上短划.

习　题

1. 将1—100，101—200，直到901—1000等每一百个数中的素数个数列成表.

2. 试求出在10001—10100范围内的素数个数.

第三章　整数的除数

§3.1　基本分解定理

一个合数 c 可表为乘积 $c=a\cdot b$，其中两个因数均不为1，且都小于 c；例如，

$$72=8\cdot 9,\qquad 150=10\cdot 15.$$

在 c 的分解式中，因数 a 与 b 中可能有一个是合数，或两个都是合数。若 a 是合数，则可进一步分解：

$$a=a_1\cdot a_2,\qquad c=a_1\cdot a_2\cdot b.$$

在上面的例子中，

$$72=2\cdot 4\cdot 9,\qquad 150=2\cdot 5\cdot 15.$$

我们可以继续分解，直到不能再分解为止；这种分解一定会在某一步停止，因为分解所得的因数变得愈来愈小，但不能是1。当不能再进一步分解时，每一个因数都是素数。这样，我们已经证明了：

每一个大于1的整数要么是素数，要么是若干个素数的乘积。

这种数的逐步分解可由许多方法来实现。我们可以利用因数表，首先求出整除 c 的最小素数 p_1，得到 $c=p_1\cdot c_1$。若 c_1 是合数，再由表求出整除 c_1 的最小素数 p_2，得到

$$c_1=p_2\cdot c_2,\qquad c=p_1\cdot p_2\cdot c_2.$$

然后，再去求 c_2 的最小素因数等等。

但是，一个重要的事实是：不管这种素因数分解如何来实现，除了这些因数的次序外，所得的结果总是一样的；即在同一个数的任意两个素因数分解式中，素数是相同的，且

每一个素数均出现相同多次。这一结果可简单地表述为：

一个数的素因数分解式是唯一的。

或许，你经常听说或使用这个所谓的"算术基本定理"，以至于你会认为它是十分显然的，但事情并非如此。这一定理可以用不同的方法来证明，但没有一个证明是显然的。我们这里所用的证明方法是归谬法(即反证法，译者注)。这个方法是这样的：假设定理不成立，然后证明这必将导致一个荒谬的结果。

证 假设我们的唯一分解定理不成立。那末一定存在一些数具有不止一个素因数分解式。在这些数中必有一个最小的，设为 c_0。通过直接验证，我们可以看出这个定理对小的整数(比如说直到10)是成立的。c_0 有最小素因数 p_0，可以写为

$$c_0 = p_0 \cdot d_0.$$

因为 $d_0 < c_0$，所以d_0 有唯一的素因数分解式①，而这意味着 c_0 的出现 p_0 的素因数分解式是唯一的。

因为根据假设，c_0 至少有两个素因数分解式，所以必有一个不出现 p_0 的分解式。设在这个分解式中的最小素数是 p_1，并记

$$c_0 = p_1 \cdot d_1. \qquad (3.1.1)$$

因为 $p_1 > p_0$，故有 $d_1 < d_0$，因而亦有 $p_0 d_1 < c_0$。 让我们来讨论数

$$c_0' = c_0 - p_0 \cdot d_1 = (p_1 - p_0) d_1. \qquad (3.1.2)$$

因为这是一个比c_0小的数，故必有唯一的分解式，因而 c_0'的素因数是由 $p_1 - p_0$ 及 d_1 的素因数所组成。因 c_0 可被 p_0 整除，故从式 (3.1.2) 推出，c_0'亦可被 p_0 整除，因此 p_0 必

---

① 显然c_0不可能是素数，所以必有$d_0 > 1$.——译者

须整除 d_1 或 $p_1 - p_0$。但因 p_1 是分解式 (3.1.1) 中的最小素数，所以 d_1 的素因数均大于 p_0。这样，唯一的可能是 p_0 整除 $p_1 - p_0$；因此它亦整除 p_1。但这是不可能的，因为素数 p_1 不能被另一素数 p_0 所整除。

上面我们说过，一个数只能以唯一的一种形式被分解为素数的乘积，这一事实决不是显然的。实际上，有许多“算术”①，在其中类似的定理并不成立。为了给出这种“算术”的一个十分简单的例子，我们来考察全体偶数

$$2, 4, 6, 8, 10, 12, \cdots.$$

这些数中有的可分解为两个偶因数的乘积，而有的则不能。后者我们可称之为偶素数。它们就是能被 2 整除但不能被 4 整除的数：

$$2, 6, 10, 14, 18, \cdots.$$

可以看出：每一个偶数，要末是一个偶素数，要末可表为偶素数的乘积。但是，这样的偶素数分解式不一定是唯一的。例如，数420有不同的偶素数分解式：

$$420 = 6 \cdot 70 = 10 \cdot 42 = 14 \cdot 30.$$

习　题

1. 写出数120，365，1970的素因数分解式。
2. 写出在 §2.1的习题中的那些数的素因数分解式.
3. 写出360的所有偶素数分解式。
4. 在什么情形下，一个偶数才有唯一的偶素数分解式？

---

① 这里我们不来解释一般的“算术”一词的含意，读者可从下面所举的例子中加以体会.——译者

§3.2 除数

让我们来分解一个数，比如说3600。分解式

$$3600=2\cdot2\cdot2\cdot2\cdot3\cdot3\cdot5\cdot5$$

可写为

$$3600=2^4\cdot3^2\cdot5^2.$$

同样地，在一般情形下，当我们分解一个数 n 时，可以把相同的素因数合并为方幂，写为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r},\qquad(3.2.1)$$

其中$p_1,p_2,\cdots,p_r$是 n 的不同的素因数，且p_1出现α_1次，p_2出现α_2次等等。一旦我们知道了形如(3.2.1)的分解式后，就能立即回答有关这个数的某些问题。

例如，我们可能要知道哪些数能整除 n。以上面提到的数3600来作为例子。假设 d 是它的一个除数，那末

$$3600=d\cdot d_1.$$

素因数分解式表明：仅有2,3,5才可能是 d 的素因数。此外，2 作为一个因数至多可能出现 4 次，而 3 与 5 每一个都至多可能出现两次。所以我们可看出，3600的可能的除数为

$$d=2^{\delta_1}\cdot3^{\delta_2}\cdot5^{\delta_3},$$

这里我们可以选择

$$\delta_1=0,1,2,3,4;\qquad\delta_2=0,1,2;\qquad\delta_3=0,1,2$$

作为指数。而这些选择可以用所有可能的方法组合起来，所以除数的个数是

$$(4+1)(2+1)(2+1)=5\cdot3\cdot3=45.$$

对具有素因数分解式(3.2.1)的任一整数 n，情况也完全相同。当 d 是 n 的一个除数，即

$$n=d\cdot d_1$$

时，能整除d的素数，只可能是那些能整除n的素数，即$p_1,\cdots,p_r$；所以d的素因数分解式可写为

$$d=p_1^{\delta_1}p_2^{\delta_2}\cdots p_r^{\delta_r}. \qquad (3.2.2)$$

素数p_1至多像在n中一样出现α_1次，对p_2及其它素数也同样。这意味着对指数δ_1我们有α_1+1种选择

$$\delta_1=0,\ 1,\ \cdots,\ \alpha_1,$$

对其它指数也同样，即对δ_2有α_2+1种选择等等。因为δ_1的α_1+1种选择中的每一个可与δ_2的α_2+1个可能的值相组合等等，由此可见，n的所有的除数的个数$\tau(n)$可由公式

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1) \qquad (3.2.3)$$

给出。

习　　题

1．一个素数有多少个除数？一个素数幂p^a呢？

2．求下列各数的除数个数：

60；366；1970；你的邮区号码。

3．在不超过100的整数中，哪个（或哪些）数的除数个数最多？

§3.3　有关除数的一些问题

$n=1$是唯一的只有一个除数的数。恰有两个除数的数是素数$n=p$，它们可被1和p整除。所以，具有两个除数的最小数是$p=2$。

让我们来考察恰有三个除数的数。根据(3.2.3)式，我们有

$$3=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1).$$

因为3是素数，所以右边仅可能有一个因数不等于1，故

$r=1$及$\alpha_1=2$。这样就有

$$n=p_1^2.$$

具有三个除数的最小数是$n=2^2=4$，把这一论证应用于除数个数是任一素数 q 的情形，我们可得到 $q=\alpha_1+1$，所以

$$\alpha_1=q-1 \quad 及 \quad n=p_1^{q-1}.$$

最小的这种数是

$$n=2^{q-1}.$$

我们再来讨论有 4 个除数的情形。这时应有

$$4=(\alpha_1+1)(\alpha_2+1),$$

而上式仅当

$$\alpha_1=3,\ \alpha_2=0, \quad 或 \quad \alpha_1=\alpha_2=1$$

时才能成立。这就导致有两个不同的解：

$$n=p_1^3, \quad n=p_1\cdot p_2.$$

有 4 个除数的最小数是$n=6$。

当有 6 个除数时，应有

$$6=(\alpha_1+1)(\alpha_2+1),$$

而上式仅当

$$\alpha_1=5,\ \alpha_2=0, \quad 或 \quad \alpha_1=2,\ \alpha_2=1$$

时才能成立。这就给出不同的解

$$n=p_1^5, \quad n=p_1^2\cdot p_2.$$

在后一种情形，当

$$p_1=2, \quad p_2=3, \quad n=12$$

时给出最小值。我们可以用这个方法去计算具有任意给定多个除数的最小整数。

有列出整数的除数个数的表，其开头几个值如下：

$n=$ 1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)=$ 1	2	2	3	2	4	2	4	3	4	2	6

你自己很容易继续写下去。

一个整数 n，如果所有比它小的数的除数个数，都比它的除数个数少，那末，我们就称它为**极大合数**。看一下我们的小表可知，开始的几个极大合数是

$$1,\ 2,\ 4,\ 6,\ 12.$$

关于这种数的性质我们知道得很少。

习　题

1. 12个战士组成的一个小队，可以用 6 种不同的形式来编队：12×1，6×2，4×3，3×4，2×6，1×12。问一个可以用 8 种，10种，12种及72种形式来编队的队伍，最少要有多少人？

2. 求出具有14个除数，18个除数及100个除数的最小整数。

3. 求出12以后的头两个极大合数。

4. 写出除数个数为两个素数乘积的所有整数。

§3.4　完全数

古希腊人十分喜欢数的玄学（有时也被称为密码学（gematry））。有这种爱好的一个很自然的理由是：希腊人用希腊字母来表示数。所以每写出一个字，一个人的名字，总是和一个数联系在一起。这样，两个人就可以比较他们的名字所表示的数的性质。

一个数的除数，或称它的除得尽的部分，在数的玄学中是特别重要的。最理想，事实上最完全的数，是那些恰由它们的所有除得尽的部分所构成的数，即所有除数的和等于这个数本身的数。这里必须指出：希腊人不把一个数的本身看

作是它的除数。

最小的完全数是

$$6 = 1 + 2 + 3.$$

下一个是

$$28 = 1 + 2 + 4 + 7 + 14,$$

再下一个是

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$$

通常，当一个数学家对某个问题找到了一个或几个特殊的解之后，他总是反复地从各个方面来考察这些解，试图发现某些规律性，从中可找出问题的一般解的线索。对于我们这几个特殊的完全数有

$$6 = 2 \cdot 3 = 2 \cdot (2^2 - 1),$$

$$28 = 2^2 \cdot 7 = 2^2 \cdot (2^3 - 1),$$

$$496 = 2^4 \cdot 31 = 2^4 \cdot (2^5 - 1).$$

这就导致下述有意义的猜测：

一个形如

$$P = 2^{p-1}(2^p - 1) = 2^{p-1} \cdot q \qquad (3.4.1)$$

的数，当

$$q = 2^p - 1$$

是麦生素数时，这个数是完全数。

事实上希腊人已经知道这一结果，并且也不难证明。可以看出，包括 P 本身在内的 P 的所有除数是

$$1,\ 2,\ 2^2,\ \cdots,\ 2^{p-1},$$

$$q,\ 2q,\ 2^2q,\ \cdots,\ 2^{p-1}q.$$

这些除数的和是

$$1 + 2 + \cdots + 2^{p-1} + q(1 + 2 + \cdots + 2^{p-1})$$

等于

$$(1+2+\cdots+2^{p-1})(q+1)=(1+2+\cdots+2^{p-1})2^p.$$

如果你不记得几何级数

$$S=1+2+\cdots+2^{p-1}$$

的和，你可以把它乘以 2 ，得到

$$2S=2+2^2+\cdots+2^{p-1}+2^p,$$

再从中减去 S 就得到

$$S=2^p-1=q.$$

这样，P 的所有的除数的和是

$$2^pq=2\cdot 2^{p-1}q.$$

因而，不包括$P=2^{p-1}q$在内的所有除数的和是

$$2\cdot 2^{p-1}q-2^{p-1}q=2^{p-1}q=P.$$

所以，我们的数是完全数。

这结果表明：每一个麦生素数给出一个完全数．在 § 2.2 中，我们已经提到，至今知道有23个麦生素数，因此也就知道了23个完全数。还有沒有其它形式的完全数呢？所有形如式(3.4.1)的完全数都是偶数，同时可以证明：如果一个完全数是偶数，那末它必有(3.4.1)式的形式。这就给我们提出了这样的问题：有沒有奇完全数？到目前为止，我们还一个也不知道。是否可能有奇完全数存在，是尚未解决的一个数论的难题。找到一个奇完全数将是一个重大的成就。因此，你可能对许多奇数去进行验证。但我们劝告你不要这样做，因为根据布赖恩特·塔克曼(Bryant Tuckerman)最近在 IBM (1968)上宣布：一个奇完全数至少要有36位数字。

习　题

利用所列出的麦生素数，计算第四、第五个完全数。

§3.5 亲和数

希腊的数的玄学的另一遗产是所谓亲和数。两个人的名字所表示的数如果具有这样的关系：一个数的各部分(除数)之和等于另一个数，且反过来也对，那末就象征着这两人之间有亲密关系。实际上希腊人仅知道唯一的一对这样的数，即

$$220 = 2^2 \cdot 5 \cdot 11, \qquad 284 = 2^2 \cdot 71.$$

它们的除数和分别为

$$1 + 2 + 4 + 5 + 10 + 20 + 11 + 22 + 55 + 110 = 284,$$

$$1 + 2 + 4 + 71 + 142 = 220.$$

费马找到了另一对亲和数

$$17296 = 2^4 \cdot 23 \cdot 47, \qquad 18416 = 2^4 \cdot 1151,$$

从而使亲和数的理论摆脱了仅仅是建立在唯一的一个例子的基础上的情况。

电子计算机特别适用于寻找亲和数对。对每一个数 n，我们让机器去确定它的所有的除数($\neq n$)及它们的和 m。然后，下一步对 m 施行同样的运算。如果经过这一运算后回到原来的数 n，那末就找到了一对亲和数(n,m)。最近，在耶鲁大学的计算机IBM7094上，对所有一百万以下的数进行了这种清查，结果找到了42对亲和数，其中有一些是新的。表2中给出了100,000以下的亲和数对。这里所提出的方法，当然也能找到完全数。如果谁愿意继续对一百万以后的数去这样做，那末，只要用更多的计算时间，肯定亦能找到一些亲和数。

表 2　100000以内的亲和数

$220=2^2\cdot5\cdot11$	$284=2^2\cdot71$
$1184=2^5\cdot37$	$1210=2\cdot5\cdot11^2$
$2620=2^2\cdot5\cdot131$	$2924=2^2\cdot17\cdot43$
$5020=2^3\cdot5\cdot251$	$5564=2^2\cdot13\cdot107$
$6232=2^3\cdot19\cdot41$	$6368=2^5\cdot199$
$10744=2^3\cdot17\cdot79$	$10856=2^3\cdot23\cdot59$
$12285=3^3\cdot5\cdot7\cdot13$	$14595=3\cdot5\cdot7\cdot139$
$17296=2^4\cdot23\cdot47$	$18416=2^4\cdot1151$
$63020=2^2\cdot5\cdot23\cdot137$	$76084=2^2\cdot23\cdot827$
$66928=2^4\cdot47\cdot89$	$66992=2^4\cdot53\cdot79$
$67095=3^3\cdot5\cdot7\cdot71$	$71145=3^3\cdot5\cdot17\cdot31$
$69615=3^2\cdot5\cdot7\cdot13\cdot17$	$87633=3^2\cdot7\cdot13\cdot107$
$79750=2\cdot5^3\cdot11\cdot29$	$88730=2\cdot5\cdot19\cdot467$

实际上，我们对亲和数的性质知道得极少，但以我们的表为基础，可提出某些猜想。例如，看来好象应该是：当亲和数愈来愈大时，这对数之比一定愈来愈接近于 1 。从表 2 还可看出，两个数可以都是偶数，也可以都是奇数，但沒有发现一个是奇数，而另一个是偶数的情形。已经在相当大的范围内寻找过这种亲和数，但是对于

$$n\leqslant 3\ 000\ 000\ 000,$$

沒有发现有这种数。

第四章　最大公因数与最小公倍数

§4.1　最大公因数

坦白地说，我们希望你将发现本章中的大部分内容是多余的。因为，它所讨论的那些概念，当你在小学学了分数计算时，就已经很熟悉了。这里讲述这些内容的理由仅在于：这样可能使你对所记得的东西有一个新的认识，以及这里的介绍，可能比你所熟悉的讲法更为系统。

我们取某个分数 a/b，即两个整数 a 与 b 的商。通常，我们总要把它化简到它的最简形式，即消去 a 与 b 的公因数。这一运算不改变分数的值，例如

$$\frac{24}{36}=\frac{8}{12}=\frac{2}{3}.$$

两个整数 a 与 b 的**公因数** d 是这样一个整数，它同时是 a 与 b 的因数，即

$$a=d\cdot a_1,\qquad b=d\cdot b_1.$$

如果 d 是 a 与 b 的公因数，那么它也能整除 $a+b$ 与 $a-b$，因为

$$a+b=a_1d+b_1d=(a_1+b_1)d,$$
$$a-b=a_1d-b_1d=(a_1-b_1)d.$$

当我们知道了 a 与 b 的素因数分解式时，就不难求出所有的公因数。我们把这两个素因数分解式写为如下的形式：

$$a=p_1^{\alpha_1}\cdots p_r^{\alpha_r},\qquad b=p_1^{\beta_1}\cdots p_r^{\beta_r}.\qquad(4.1.1)$$

这里我们允许把这两个分解式写得好象 a 和 b 有相同的素因数

$$p_1,\ p_2,\ \cdots,\ p_r,$$

但约定可以出现零指数。例如，若 p_1 整除 a 但不整除 b，那末，在（4.1.1）式中，令 $\beta_1 = 0$。这样，若

$$a = 140, \qquad b = 110. \qquad (4.1.2)$$

就写为

$$a = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^0, \qquad b = 2^1 \cdot 5^1 \cdot 7^0 \cdot 11^1. \qquad (4.1.3)$$

在(4.1.1)式中，a 的因数 d 仅可能以出现在 a 中的 p_i 作为其素因数，且 p_i 在 d 中的指数 δ_i 不能超过 a 中的相应的指数 α_i。对 b 的任一因数，以上的条件也成立。所以 a 与 b 的公因数 d，仅可能以同时出现在 a 与 b 中的 p_i 作为其素因数，且 p_i 在 d 中的指数 δ_i 不会超过指数 α_i 和 β_i 中的较小者。

根据这一讨论，我们得出：

任意两个整数 a 与 b，必有一个**最大公因数** d_0。d_0 的素因数 p_i，就是同时出现在 a 与 b 中的那些素因数，且 p_i 在 d_0 中的指数，就是 α_i 与 β_i 中较小的一个。

例 取(4.1.2)式中的这两个数，它们的素因数由式(4.1.3)给出。可看出

$$d_0 = 2^1 \cdot 5^1 = 10.$$

由于最大公因数中的素因数 p_i 的指数，至少同它在任一其它的公因数中的指数一样大，我们就得到了最大公因数的特征性质①：

任一公因数 d 一定整除最大公因数 d_0。

两个数的最大公因数(缩写为 g.c.d.）是如此重要，以至于有必要给它一个专门的记号：

---

① 具有这样性质的数一定是最大公因数.——译者

$$d_0=(a,b). \tag{4.1.4}$$

习　　题

1．求下列各对数的最大公因数：

(a) 360与1970；　　(b) 30与365；

(c) 你的电话号码与你的邮区号码。

2．你怎样来证明$\sqrt{2}$是无理数？素因数分解式的唯一性定理怎样应用于这一证明及相类似的证明中？

§4.2　互素数

数 1 是任意一对数 a 与 b 的公因数。可以出现数 1 是唯一的公因数的情形，这就使得

$$d_0=(a,b)=1. \tag{4.2.1}$$

在这种情形下，我们就说 a 和 b 是**互素的**。

例　$(39,22)=1$。

如果这两个数有一个大于 1 的公因数，那末，它们也必有一个公共的素因数；所以两个数仅当它们沒有公共的素因数时，才是互素的。因此，条件(4.2.1)意味着 a 与 b 沒有公共的素因数，即它们所有的素因数是不同的。

让我们回到本章开始所说的，把一个分数 a/b 化简到最简形式的问题。若 d_0 是 a 和 b 的 g.c.d.，则可写为

$$a=a_0d_0,\qquad b=b_0d_0. \tag{4.2.2}$$

这时有

$$\frac{a}{b}=\frac{a_0d_0}{b_0d_0}=\frac{a_0}{b_0}. \tag{4.2.3}$$

在式(4.2.2)中，a_0 与 b_0 不可能有公共的素因数，若不然，a 与 b 就将有一个大于 d_0 的公因数。因此得到

$$(a_0,b_0)=1。\qquad (4.2.4)$$

这意味着式(4.2.3)中的第二个分数是 a/b 的最简形式，不能再进一步化简了。

经常用到的互素数的一个性质是：

除法规则 **若乘积 ab 可被 c 整除，c 和 b 互素，则 a 可被 c 整除。**

证 因为 c 整除 ab，所以 c 的素因数必出现于 a 与 b 的素因数中。但由于 $(b,c)=1$，所以不能出现于 b 中。这样，c 的全部素因数整除 a，但不整除 b，又因为 c 整除 ab，所以，出现在 a 中的方次不会小于在 c 中的方次。

下面，我们将用到另一个事实：

若两个互素数的乘积是一个平方数，

$$ab=c^2,\qquad (a,b)=1,\qquad (4.2.5)$$

那末，a 和 b 都是平方数：

$$a=a_1^2,\qquad b=b_1^2。\qquad (4.2.6)$$

证 一个数是平方数的必要和充分的条件是其素因数分解式中的所有指数均为偶数。因为在式(4.2.5)中，a 与 b 互素，所以 c^2 中任一素因数不出现于 a 中，就出现于 b 中，但不可能同时出现于二者之中。因而，在 a 与 b 的素因数分解式中，素因数的指数一定是偶数。

习　题

1. 哪些数与 2 互素？

2. 为什么对两个相邻整数 n 与 $n+1$ 必有

$$(n,n+1)=1。$$

3. 检查 §3.5 中的表 2 所列出的亲和数对，找出那些互素的亲和数对。

4. 由式(4.2.5)及(4.2.6)所表述的规则，当用任意次幂去代替平方时是否成立?

§4.3 欧几里得算法

让我们再回到分数 a/b。若 $a>b$，这个分数就大于1，我们经常把它分为一个整数部分和一个小于1的眞分数。

例 我们写

$$\frac{32}{5}=6+\frac{2}{5}=6\frac{2}{5}, \qquad \frac{63}{7}=9+\frac{0}{7}=9.$$



图 4.3.1

在一般情形下，我们利用两个整数 $a\geqslant b$ 的(不完全)除法来做到这一点：我们可以写

$$a=qb+r, \qquad 0\leqslant r\leqslant b-1. \qquad (4.3.1)$$

为了指出这样写总是可能的，我们把整数 $0,1,2,\cdots$ 表示在数轴上（图4.3.1）。数 a 被表示在这数轴的某一点处。我们从0开始，依次标出 b，$2b,3b$ 等等，直到这样的 qb，使得 qb 不大于 a，而 $(q+1)b$ 大于 a。从 qb 到 a 的距离就是 r。我们称 r 为除法(4.3.1)中的余数，q 为(不完全)商。这个商 q 是如此经常出现，以至有必要给它一个专门的符号：

$$q=\left[\frac{a}{b}\right],$$

这一符号表示不超过 a/b 的**最大整数**。对上面的例子，我们有

$$\left[\frac{32}{5}\right]=6, \quad \left[\frac{63}{7}\right]=9.$$

在上一节中，我们讨论了两个整数 a 与 b 的 g.c.d.

$$d_0=(a,b). \tag{4.3.2}$$

那里为了求出 d_0，我们假定了已知 a 与 b 的素因数分解式.对于大的数来说，要得到这些分解式可能是一项艰巨的工作.还有一个重要的，十分不同的方法可以用来求出g.c.d.，这个方法不依赖于这些分解式，而是基于以下的结论：

若 $a=qb+r$，$0\leqslant r\leqslant b-1$，则

$$(a,b)=d=(r,b). \tag{4.3.3}$$

证 我们记

$$d_0=(a,b), \quad d_1=(r,b),$$

这样，所要证明的关系式就变为 $d_0=d_1$. a 与 b 的任一公因数亦整除

$$r=a-qb,$$

因此 d_0 整除 r. 因为 d_0 是 r 的因数，也是 b 的因数，所以它必整除 $d_1=(b,r)$，因此 $d_1\geqslant d_0$. 另一方面由(4.3.1)知，r 和 b 的任一公因数整除 a，所以 d_1 整除 a. 因为 d_1 也是 b 的因数，故它必整除 $d_0=(a,b)$，所以 $d_0\geqslant d_1$. 这就证明了 $d_0=d_1$.

例 $1066=5\cdot 200+66$，因此$(1066,200)=(66,200)$.

由关系式(4.3.3)所表述的结果，给出了一个计算两个数的g.c.d.的简单方法. 代替求 a 与 b 的g.c.d.，我们只要去求 r 与 b 的g.c.d.. 这应该是比较简单的，因为 r 是一个比 a 与 b 都要小的数. 我们可用同样的方法去求 r 与 b 的g.c.d.，即用 r 去除 b 得

$$b=q_1r+r_1,$$

这里 r_1 比 b 与 r 都小。根据公式(4.3.3)得到

$$d_0=(a,b)=(b,r)=(r,r_1).$$

再对 r 与 r_1 作同样的讨论。依此下去，结果就得到了一串数对，每一对数有相同的最大公因数：

$$d_0=(a,b)=(b,r)=(r,r_1)=(r_1,r_2)=\cdots. \quad (4.3.4)$$

因为这些余数不断减小，所以一定会出现一个余数 $r_{k+1}=0$，而这一串数对也就到此为止。

这一情形出现于除法

$$r_{k-1}=q_{k+1}r_k+0$$

所以 r_k 整除 r_{k-1}。这时有

$$(r_{k-1},r_k)=r_k,$$

由此及(4.3.4)就证明了

$$d_0=(a,b)=r_k.$$

换句话说，d_0 等于第一个这样的余数 r_k，它整除它的前一个余数。

例 让我们来求数1970与1066的g.c.d.。当我们用一个数去除另一个数，并象上面一样继续做下去时，就得到：

$$1970=1\cdot1066+904,$$
$$1066=1\cdot904+162,$$
$$904=5\cdot162+94,$$
$$162=1\cdot94+68,$$
$$94=1\cdot68+26,$$
$$68=2\cdot26+16,$$
$$26=1\cdot16+10,$$
$$16=1\cdot10+6,$$
$$10=1\cdot6+4,$$
$$6=1\cdot4+2,$$

$$4=2\cdot 2+0.$$

因此，$(1970,1066)=2$。

这种求两个数的g.c.d.的方法称为欧几里得算法，因为这一方法最早的记述是在欧几里得的原本中出现的。这个方法特别适用于机器计算。

习　　题

1. 用欧几里得算法来解§4.1中的习题。

2. 求最初四对亲和数中的每一对数的g.c.d.，并把所得的结果与从素因数分解式所得的结果相对照，检查所得的结果。

3. 求数

$$n!=1\cdot 2\cdot 3\cdot\cdots\cdot n$$

的十进制表示中结尾有多少个零。用阶乘表检查所得的结果。

§4.4　最小公倍数

让我们再回到分数上来。为了把两个分数

$$\frac{c}{a},\quad \frac{d}{b}$$

相加（或相减），我们要把它们化为具有相同的分母的形式，然后把分子相加（或相减）。

例

$$\frac{2}{15}+\frac{5}{9}=\frac{6}{45}+\frac{25}{45}=\frac{31}{45}.$$

一般地，为了求出和

$$\frac{c}{a}+\frac{d}{b},$$

我们必须求出 a 与 b 的一个公倍数，即一个数 m，它可以同时被 a 与 b 整除。它们的乘积 $m=ab$。显然是一个这样的数，所以对于分数的和我们有

$$\frac{c}{a}+\frac{d}{b}=\frac{cb}{ab}+\frac{da}{ab}=\frac{cb+da}{ab}.$$

但是还有无穷多个其它的 a 与 b 的公倍数。再假设我们知道这两个数的素因数分解式

$$a=p_1^{\alpha_1}\cdots p_r^{\alpha_r},\qquad b=p_1^{\beta_1}\cdots p_r^{\beta_r}. \qquad (4.4.1)$$

一个可以同时被 a 与 b 整除的数 m，必须被 a 与 b 中的每一个素因数 p_i 的 μ_i 次方整除，μ_i 不小于两个指数 α_i 和 β_i 中的较大者。这样一来，在公倍数 m 中有一个最小的

$$m_0=p_1^{\mu_1}\cdots p_r^{\mu_r}, \qquad (4.4.2)$$

这里每一个指数 μ_i 等于 α_i 与 β_i 中的较大者。这表明 m_0 是**最小公倍数**（简记作 l.c.m.），且 a 与 b 的任一其它的公倍数必可被 m_0 所整除。对这个 l.c.m. 有一个专门的记号

$$m_0=[a,b]. \qquad (4.4.3)$$

例 $a=140,\quad b=110.$

这两个数的素因数分解式是

$$a=2^2\cdot5^1\cdot7^1\cdot11^0 \text{ 及 } b=2^1\cdot5^1\cdot7^0\cdot11^1,$$

因此 $[a,b]=2^2\cdot5^1\cdot7^1\cdot11^1=1540.$

在 g.c.d. 和 l.c.m. 之间存在下面的简单关系式：

$$ab=(a,b)[a,b]. \qquad (4.4.4)$$

证 当我们把式(4.4.1)中的两个数相乘时，得到

$$ab = p_1^{\alpha_1+\beta_1}\cdots p_r^{\alpha_r+\beta_r}. \qquad (4.4.5)$$

正如我们已经指出的，在(a,b)中素数p_i的指数是两个数α_i和β_i中的较小者；而在$[a,b]$中则是较大者。不妨设$\alpha_i \leqslant \beta_i$。这时，$p_i$在$(a,b)$中的指数是$\alpha_i$，而在$[a,b]$中是$\beta_i$。因此在它们的乘积

$$(a,b)\cdot[a,b]$$

中p_i的指数是$\alpha_i+\beta_i$，即正好与乘积(4.4.5)中p_i的指数相同。这就证明了关系式(4.4.4)成立。

例

$a = 140,\quad b = 110,\quad (a,b) = 10,\quad [a,b] = 1540;$

$$ab = 140\cdot 110 = 10\cdot 1540 = (a,b)\cdot[a,b].$$

从公式(4.4.4)可看出，若a与b互素，那末它们的乘积等于它们的l.c.m.。因为这时$(a,b)=1$，所以

$$ab = [a,b].$$

习　题

1. 求§4.1习题中的那些数对的l.c.m.。
2. 求最初四对亲和数中每一对数的l.c.m.。

第五章　毕达哥拉斯问题

§5.1　预备知识

在引言(§1.3)中，我们提到了最古老的数论问题之一：求出所有边长为整数的直角三角形，即求方程

$$x^2+y^2=z^2 \tag{5.1.1}$$

的所有整数解。

这个问题可以利用整数的简单性质来解决。但在求解之前，我们先作一些预备性的讨论.满足方程(5.1.1)的三个整数所组成的集合

$$(x,y,z) \tag{5.1.2}$$

称为**毕达哥拉斯三元数组**。我们不考虑三角形有一边为零的这种显然情形。

显然，若(5.1.2)是一个毕达哥拉斯三元数组，那末，每个数乘上整数 k 后，所得的任一三元数组

$$(kx,ky,kz) \tag{5.1.3}$$

也是一个毕达哥拉斯三元数组，且反之亦然。这样一来，在求解时，只要求出所谓**本原三角形**就足够了；本原三角形是三边没有公因数 $k(>1)$的三角形。例如，

$$(6,8,10),\quad (15,20,25)$$

都是由本原解(3,4,5)所生成的毕达哥拉斯三元数组。

在**本原三元数组**(x,y,z)中，这三个数没有公因数.事实上，我们可以给出一个更强的定义：**在本原三元数组中，任意两个数均没有公因数**，即

$$(x,y)=1,\quad (x,z)=1,\quad (y,z)=1. \tag{5.1.4}$$

为了证明这一点，我们先假设，例如，x 与 y 有公因数。那末，它们就有一个公共的素因素 p。根据式(5.1.1)，p 一定也整除 z，这样一来，(x,y,z)就将不是一个本原三元数组了。对式(5.1.4)中的另外两个条件可作同样的论证。

关于本原三元数组中的数的性质，还可以说得更多些。我们已经知道 x 与 y 不能同时为偶数。但我们还可证明 x 与 y 不能同时为奇数。假定

$$x=2a+1,\quad y=2b+1.$$

我们把这两个数平方后再相加，得到

$$\begin{aligned} x^2+y^2 &= (2a+1)^2+(2b+1)^2 \\ &= 2+4a+4a^2+4b+4b^2 \\ &= 2+4(a+a^2+b+b^2), \end{aligned}$$

这个数可被 2 整除但不能被 4 整除。根据式(5.1.1)，这意味着 z^2 可被 2 整除，但不能被 4 整除，而这是不可能的。因为若 z^2 被 2 整除，则 z 被 2 整除，所以 z^2 被 4 整除。

因为数 x 与 y 中一个是偶的，另一个是奇的，所以 z 也是奇的。我们将假定：*在以下的记号中，x 是偶的，而 y 是奇的。*

§5.2 毕达哥拉斯方程的解

为求出毕达哥拉斯方程(5.1.1)的本原解，我们把它写为

$$x^2=z^2-y^2=(z+y)(z-y). \qquad (5.2.1)$$

由于 x 是偶的，而 y 和 z 是奇的，所以三个数

$$x,\quad z+y,\quad z-y$$

都是偶的。这样，式(5.2.1)两边可同除以 4，并得到

$$\left(\frac{1}{2}x\right)^2=\frac{1}{2}(z+y)\cdot\frac{1}{2}(z-y). \qquad (5.2.2)$$

我们令

$$m_1 = \frac{1}{2}(z+y), \qquad n_1 = \frac{1}{2}(z-y), \qquad (5.2.3)$$

式(5.2.2)就变为

$$\left(\frac{1}{2}x\right)^2 = m_1 n_1. \qquad (5.2.4)$$

式(5.2.3)中的数 m_1 与 n_1 是互素的。为了看出这一点，假设

$$d = (m_1, n_1)$$

是 m_1 与 n_1 的 g.c.d.。这时，正如我们在§4.1提到的，d 必定同时整除整数

$$m_1 + n_1 = z, \qquad m_1 - n_1 = y.$$

但在本原三元数组中，z 与 y 的唯一的公因数是1，所以，

$$d = (m_1, n_1) = 1. \qquad (5.2.5)$$

因为由式(5.2.4)知，这两个互素数的乘积是一个平方数，所以我们利用在§4.2结束时所给出的结果，就知道整数 m_1 与 n_1 都是平方数

$$m_1 = m^2, \qquad n_1 = n^2, \qquad (m, n) = 1. \qquad (5.2.6)$$

不失一般性，这里可取 $m>0$，$n>0$。现在，我们在方程(5.2.3)和(5.2.4)中，分别用 m^2 和 n^2 来代替 m_1 与 n_1，得到

$$m^2 = \frac{1}{2}z + \frac{1}{2}y, \qquad n^2 = \frac{1}{2}z - \frac{1}{2}y,$$

$$m^2 n^2 = \frac{1}{4}x^2,$$

所以，

$$x = 2mn, \quad y = m^2 - n^2, \qquad z = m^2 + n^2. \qquad (5.2.7)$$

直接验证可知，这三个数总满足毕达哥拉斯关系式

$$x^2+y^2=z^2.$$

剩下来的只是要去确定，哪些正整数 m 与 n 确实对应于本原三角形。我们将证明以下的三个条件是必要和充分的。

$$\left.\begin{array}{l}(1)\ (m,n)=1;\\(2)\ m>n;\\(3)\ m\text{与}n\text{中一个是偶的，另一个是奇的。}\end{array}\right\}(5.2.8)$$

证 首先我们来证明：若 x,y,z 构成一个本原三元数组，那末条件(5.2.8)成立。我们已经证明，条件(1)是 x,y,z 互素的一个推论。条件(2)可从 x,y,z 都是正数推出。为了证明条件(3)是必要的，我们注意到，若 m 与 n 两个都是奇的，则根据式(5.2.7)知，y 与 z 将都是偶数，而这与上节结束时推出的结果相矛盾。

反之，若条件(5.2.8)满足，则式(5.2.7)就确定了一个本原三元数组：条件(2)保证了 x,y,z 都是正的。它们中的任意两个会不会有公共的素因数 p 呢？因为它们满足 $x^2+y^2=z^2$，所以整除它们之中两个数的素数 p，一定亦整除第三个数。当 p 整除 x 时，由式(5.2.7)知，它必整除 $2mn$；根据条件(3)与式(5.2.7)，y 与 z 都是奇的，所以 p 不等于2。假设 $p\neq2$ 是整除 m 的奇素数，那末条件(1)与式(5.2.7)表明 p 不能整除 y 与 z。同样的论证可以应用于假定 p 整除 n 的情形。

找出了为使 m 与 n 给出一个本原三角形的必要和充分条件后，从表达式(5.2.7)就可得到所有这种三角形。例如，若取

$$m=11,\quad n=8,$$

那末我们的条件被满足，且得到

$$x=176, \quad y=57, \quad z=185.$$

在表 3 中，我们给出了对应于最初的一些值 m 与 n 的所有的本原三角形。

表 3

n \ m	2	3	4	5	6	7
1	4, 3, 5		8,15,17		12,35,37	
2		12,5,13		20,21,29		28,45,53
3			24,7,25			
4				40,9,41		56,33,65
5					60,11,61	
6						84,13,85

习 题

1. 把表 3 扩充到包括所有 $m\leqslant 10$的值。

2. 能不能有两组满足条件(5.2.8)的不同的值 m，n，给出同样的三角形。

3. 求出斜边$\leqslant 100$的所有毕达哥拉斯三角形.

§5.3 与毕达哥拉斯三角形有关的一些问题

我们已经解决了求所有毕达哥拉斯三角形的问题。在数学中几乎总是这样，一个问题的解决就导致另外一些问题的解决，而新的问题常常可能比原来的问题困难得多。这里也是如此。

与本原三角形有关的一个自然的问题是：当直角三角形

中的一边已经给出时，如何去求另外两边？首先考虑 y 边是已知的情形。根据(5.2.7)式，

$$y=m^2-n^2=(m+n)(m-n), \qquad (5.3.1)$$

其中 m 与 n 满足条件(5.2.8)。式(5.3.1)中的两个因数$(m+n)$与$(m-n)$是互素的。为证明这一点，我们注意到，由于m，n是一奇一偶，所以这两个因数

$$a=m+n, \qquad b=m-n \qquad (5.3.2)$$

都是奇数。若 a 与 b 有一个公共的奇素因数 p，那么 p 应该同时整除

$$a+b=m+n+(m-n)=2m$$

及

$$a-b=m+n-(m-n)=2n,$$

所以 p 应该同时整除 m 与 n .但因$(m,n)=1$，这是不可能的。

现在假设所给的奇数 y 有这样的两个因数的分解式

$$y=ab, \quad a>b, \quad (a,b)=1. \qquad (5.3.3)$$

从(5.3.2)我们得到

$$m=\frac{1}{2}(a+b), \qquad n=\frac{1}{2}(a-b). \qquad (5.3.4)$$

这两个数也是互素的，因为它们的任一公因数必将整除 $a=m+n$ 及 $b=m-n$。此外，m 与 n 不能都是奇数，因为这样的话，a 与 b 将均可被 2 整除。这就证明了 m 与 n 满足条件(5.2.8)，因而就确定了一个本原三角形，它的一边是

$$y=m^2-n^2.$$

例 设 $y=15$。我们有两个形如(5.3.3)的分解式，即

$$y=15\cdot1=5\cdot3.$$

由第一个分解式给出

$$m=8, \quad n=7, \quad x=112, \quad y=15, \quad z=113;$$

而由第二个给出

$$m=4,\quad n=1,\quad x=8,\quad y=15,\quad z=17.$$

其次，设 x 边为已知。因为 m 与 n 中必有一个可被 2 整除，所以从 $x=2mn$ 可看出，x 必须被 4 整除。如果把 $x/2$ 分解为两个互素的因数的乘积，那末，就可把较大的一个取作为 m，较小的一个为 n。

例 取 $x=24$。有

$$\frac{1}{2}x=12\cdot 1=4\cdot 3.$$

由第一个分解式给出

$$m=12,\quad n=1,\quad x=24,\quad y=143,\quad z=145;$$

而由第二个给出

$$m=4,\quad n=3,\quad x=24,\quad y=7,\quad z=25.$$

第三，也是最后一种情形，将引导我们去触及数论中的一些重要问题。如果 z 是本原毕达哥拉斯三角形的斜边，那末，根据(5.2.7)式有

$$z=m^2+n^2,\tag{5.3.5}$$

即 z 应该是满足条件(5.2.8)的两个数 m 与 n 的平方和。

这就导致我们去提出一个已被费马所解决的问题：什么时候一个整数可表为两个平方数之和

$$z=a^2+b^2\ ?\tag{5.3.6}$$

暂时我们对 a 与 b 不加任何限制，它们可以有公因数，以及它们中的一个或全部可以是零。在不超过10的整数中，以下的几个数是两个平方数之和：

$$0=0^2+0^2,\quad 1=1^2+0^2,\quad 2=1^2+1^2,\quad 4=2^2+0^2,$$
$$5=2^2+1^2,\quad 8=2^2+2^2,\quad 9=3^2+0^2,\quad 10=3^2+1^2.$$

其余的数3,6,7不能表为两个平方数之和。

下面我们来叙述：怎样判定一个数是不是两个平方数之和。遗憾的是，它的证明不是简单的，这里只能略去不讲。

首先，我们来讨论素数。每一个形如 $p=4n+1$ 的素数，一定是两个平方数之和。例如，

$$5=2^2+1^2,\qquad 13=3^2+2^2,$$
$$17=4^2+1^2,\qquad 29=5^2+2^2.$$

一个令人惊异的事实是：这种表示式是唯一的。

其余的奇素数是 $q=4n+3$ 的形式。因此，

$$q=3,\ 7,\ 11,\ 19,\ 23,\ 31,\ \cdots.$$

没有一个这样的素数可表为两个平方数之和。事实上，没有一个形如$4n+3$的数是两个平方数之和。为了证明这一点，我们注意到：若 a 与 b 都是偶数，则 a^2 与 b^2 均可被 4 整除，所以 a^2+b^2也被 4 整除；若 a 与 b 都是奇数，比如设

$$a=2k+1,\quad b=2l+1,$$

那末，
$$a^2+b^2=4k^2+4k+1+4l^2+4l+1$$
$$=4(k^2+l^2+k+l)+2,$$

所以 a^2+b^2 被 4 除后，余数为 2；最后，若整数 a，b 是一偶一奇，设 $a=2k+1, b=2l$，那末，

$$a^2+b^2=4k^2+4k+1+4l^2,$$

所以 a^2+b^2 被 4 除后余数为 1。因为这里列举出了所有的可能性，所以我们证明了：两个平方数之和不可能是$4n+3$的形式。

再注意到$2=1^2+1^2$，这就完成了对所有素数的考察。

验证一个合数 z 是不是两个平方数之和，可按如下的方法进行：设 z 的素因数分解式是

$$z=p_1^{\alpha_1}\ p_2^{\alpha_2}\cdots. \tag{5.3.7}$$

那末，当且仅当每一个形为$4n+3$的 p_i 的指数为偶数时，z

才是两个平方数之和。

例

$$z=198=2\cdot3^2\cdot11$$

不是两个平方数之和，因为11是$4n+3$形式的素数且是一次幂。

$$z=194=2\cdot97$$

是两个平方数之和，因为它的两个素因数都不是$4n+3$的形式。我们可求得

$$z=13^2+5^2.$$

让我们回到原来的问题上：确定所有的数z，使它可以作为本原毕达哥拉斯三角形的斜边。这样的数z必定有表达式$z=m^2+n^2$，其中m与n满足条件（5.2.8）.可以证明：z为这种情形的必要和充分的条件是，z的所有的素因数是$p=4n+1$的形式。同样，我们略去其证明。

例 1）$z=41$。这里可求出唯一的一个把z表示为两个平方数之和的表示式

$$z=5^2+4^2,$$

所以，

$$m=5,\quad n=4;\qquad x=40,\quad y=9,\quad z=41$$

就是所对应的三角形。

2）$z=1105=5\cdot13\cdot17$.我们有四个把z表为两个平方数之和的表示式

$$1105=33^2+4^2=32^2+9^2=31^2+12^2=24^2+23^2.$$

我们留给读者去求出相应的三角形。

关于毕达哥拉斯三角形的各种问题，可以利用我们的公式(5.2.7)

$$x=2mn,\qquad y=m^2-n^2\qquad z=m^2+n^2$$

去解决。例如，我们可以问，如何去求一个具有给定面积 A 的毕达哥拉斯三角形。如果这个三角形是本原的，那末它的面积是

$$A=\frac{1}{2}xy=mn(m-n)(m+n). \qquad (5.3.8)$$

这里四个因数中，有三个是奇的。不难看出，它们是两两互素的。所以，为了求出所有可能的 m 与 n 的值，我们可以先挑选 A 的两个互素的奇因数 k，l $(k>l)$，并令

$$m+n=k, \qquad m-n=l,$$

这给出

$$m=\frac{1}{2}(k+l), \qquad n=\frac{1}{2}(k-l).$$

然后，再验证这些值是否确实满足条件(5.3.8)。

注意到下面的事实，可使这一讨论稍为简单些。这就是仅在特殊情形

$$m=2, \quad n=1, \quad A=6$$

下，才能使(5.3.8)式的因数中有两个等于1。因为，这时唯一的可能的形式是

$$n=m-n=1,$$

而这就给出了上面的数值。

例 求所有面积 $A=360$ 的毕达哥拉斯三角形。A 的素因数分解式是

$$A=2^3\cdot 3^2\cdot 5.$$

把 A 写为四个两两互素的因数的乘积的唯一方法是

$$A=8\cdot 1\cdot 5\cdot 9,$$

所以一定有 $m+n=9$。这不能给出一个所需要的三角形：若 $m=8$，则 $n=1$，而 $m-n=7$ 不能整除 A。另一种情形是 $n=8$，

$m=1$，而这是为所需要满足的条件$m>n$所排除的。

以上的结论，并未排除有一个非本原三角形具有$A=360$的可能性。以下的论证，可以用于在一般情形下，去确定是否具有给定面积的非本原三角形。若

$$dx, \quad dy, \quad dz$$

是边长具有公因数d的三角形的三边，那末，它的面积是

$$A=\frac{1}{2}\cdot dx\cdot dy=d^2mn(m-n)(m+n).$$

所以d^2是A的因数，而且，如果d是三边长的g.c.d.，那末，

$$A_0=\frac{A}{d^2}=mn(m-n)(m+n)$$

一定是一个本原三角形的面积。

我们来继续讨论。刚才讨论了$A=360$的情形，这个数有三个平方因数

$$d_1=4, \quad d_2=9, \quad d_3=36.$$

相应地可得

$$\frac{A}{d_1}=90=2\cdot3^2\cdot5, \quad \frac{A}{d_2}=40=2^3\cdot5, \quad \frac{A}{d_3}=10=2\cdot5.$$

40或10均不可能表为四个两两互素的因数的乘积，而对90只有一种这样的表法，即

$$90=1\cdot2\cdot3^2\cdot5.$$

(除去情形$m=2,n=1,A=6$外，四个因数中至多可能有一个为1.)因为9是最大的因数，所以必须取$m+n=9$。从所有可能的选择$m=1,2,5$分别得到$n=8,7,4$，而仅有$m=5$，$n=4$满足条件$m>n$,但在这种情况下，$mn(m+n)(m-n)\neq$

90。所以，我们得到结论：沒有一个毕达哥拉斯三角形，本原的或不是本原的，其面积 $A=360$。

我们还可以问许多其它的问题，但我们只再提出一个。一个三角形的周长是

$$c=x+y+z; \qquad (5.3.9)$$

对于本原毕达哥拉斯三角形，其周长是

$$c=2mn+(m^2-n^2)+(m^2+n^2)=2m(m+n).$$

我们把提出某个方法，用以求出所有具有给定周长的毕达哥拉斯三角形的这一工作，留给读者。请不要忘记，把这一方法应用于一些数值例子上。

我们已经解决了作出所有毕达哥拉斯三角形的问题。这引导我们去研究更一般的有关问题。一个自然的推广，是研究所谓**赫伦三角形**，这是以希腊亚历山大时期的数学家赫伦(Heron)的名字命名的。和以前一样，在这些三角形中，我们要求边长 x,y,z 是整数，但是我们放弃一个角是 $90°$ 的条件，而代之以要求面积是整数。显然，毕达哥拉斯三角形属于这一类。

验证一个给定的三角形是不是赫伦三角形，最简单的办法是利用三角形面积的赫伦公式

$$A=\sqrt{\frac{1}{2}c\left(\frac{1}{2}c-x\right)\left(\frac{1}{2}c-y\right)\left(\frac{1}{2}c-z\right)},$$

这里 c 是我们在(5.3.9)式中定义的周长。虽然，我们知道很多很多的赫伦三角形，但是我们还沒有一个给出它们全体的一般公式。这里是开头几个这种(非直角)三角形的例子：

$$x=7, \quad y=15, \quad z=20;$$

$$x=9, \quad y=10, \quad z=17;$$

$$x=13, \quad y=14, \quad z=15;$$

$$x=39,\quad y=41,\quad z=50。$$

在结束对毕达哥拉斯三角形的讨论之前，我们不能不提到数学中最著名的问题之一——费马猜想：对 $n>2$，不存在正整数 x,y,z，使得

$$x^n+y^n=z^n。$$

这一思想是费马在精读希腊数学家丢番图的著作《算术》一书的译本时产生的。这一著作主要是讨论这样一些问题：在这些问题中，需要应用有关毕达哥拉斯三角形的一些公式。费马把他的评注写在了书页的空白处。

费马对他的"发现"极为高兴，并相信他已经有了一个奇妙的证明，但遗憾的是空白处太小，而不能把证明写下来。从那时候起，数学家就一直对此感到怀疑。为了找到一个证明，已经提出了一些最巧妙的方法，这种探索的结果产生了一些新的数学基础理论。利用理论与计算机相结合，费马定理已经对许多指数 n 得到了证明；现在我们知道对所有的 n，$3\leqslant n\leqslant 4002$，这个结果是正确的①。

由于在几个世纪中，一些最杰出的数学家，在寻求一个一般的证明中都遭到了失败，现在普遍的看法是，尽管费马的技巧是不用争辩的，但他一定是由于自己一时糊涂而受骗了。看来，不管他的空白处有多大，他的证明也不会是正确的。

当然，你有权利去进行你自己的尝试，但必须告诫你的是：在数学中，没有一个定理有如此多的错误的证明，其中只有很少一些出自优秀数学家之手，而不计其数的则完全是

① 1976年已经有人证明，费马定理对所有 $n<10^5$ 是成立的。1983 年 G. Faltings 证明了对任给的 $n\geqslant 3$，必存在和 n 有关的整数 $z_0=z_0(n)$，使当 $z>z_0$ 时 $x^n+y^n=z^n$ 无整数解，但这 z_0 目前还不能具体计算出来。——译者

胡思乱想。“费马大定理”的证明，继续出现在寄给知名数论专家的邮件中，其中大多数还附有信件，要求立即承认其证明，并付给现已不值钱的奖金，这一奖金是过去由一位德国数学家作为奖赏一个正确的证明而设立的。

习　　题

1. 求出一边长等于(a)50；(b)22的所有的毕达哥拉斯三角形。

2. 利用一个数可以表为两个平方数之和的判别法，来确定数

$$100,\ 101,\ \cdots,\ 110$$

中，哪些有这样的表示式。对有表示式的求出其所有的表示式。这些数中哪些可作为一个本原毕达哥拉斯三角形的斜边？

3. 有沒有面积为

$$A=78,\quad A=120,\quad A=1000$$

的毕达哥拉斯三角形？

4. 求出所有周长为

$$c=88,\quad c=110$$

的毕达哥拉斯三角形。

第六章　记　数　法

§6.1　成千成万的数

古代的毕达哥拉斯学派认为，万物皆为数。然而，他们的数的宝库比起现在日常生活中包围着我们的各种各样奇形怪状的数字来要稀少得多。我们计算各种巨大的数目，同时我们自己也和各种各样的巨大数目相联系着。我们的生活离不开社会安全号码，邮区号码，账号，电话号码，房间号码以及门牌号码等等。每日见到的是无数的账单，支票，赊账以及结算等。公共预算达到数十亿；大量的统计数字是一种易于接受的论证形式。到处是把各种数据飞速地送进计算机，用它来分析大企业的经营方针；跟踪人造卫星的轨道；以及研究处在每十亿分之一秒内就发生很多次相互作用的高速状态下的原子核的内部情况。

一旦当人们所遇到的数大到无法用手指来计算时，就产生了系统计数的要求。目前的一切都是从这种想法开始，不断发展而来的。已经有种种不同的方法用来把数分组，它们中的大多数一旦被证明不如其它的计算系统好时，就被抛弃不用了。幸运的是，我们现在的十进制——基于把数按十个来分组——至今已被十分普遍地接受了。对于我们研究数来说，十进制在某些方面显出是一种意外方便的记数法。

这里不必为你详细地讲述记数法。因为在最初二学年的训练之后，使得我们在后来的一生中，几乎本能地知道一串数字所代表的数是什么。例如

$$75 = 7 \cdot 10 + 5,$$

$$1066 = 1 \cdot 10^3 + 0 \cdot 10^2 + 6 \cdot 10 + 6,$$
$$1970 = 1 \cdot 10^3 + 9 \cdot 10^2 + 7 \cdot 10 + 0.$$

一般地，在以10为基数的记数法中，一串数字

$$a_n a_{n-1} \cdots a_2 a_1 a_0 \qquad (6.1.1)$$

表示数

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \qquad (6.1.2)$$

这里，系数或数字 a_i 取下列数值之一：

$$a_i = 0, 1, \cdots, 9. \qquad (6.1.3)$$

数 $b = 10$ 称为此记数法的基。

这种印度-阿拉伯数系，在公元1200年左右从东方传入欧洲，自此以后，对这种数系一直沒有引起过争议。这种记数法被称为位置记数法，因为任何一个数字的位置决定它的值。由于对符号 0 的无害而巧妙的利用，使得表示一个空位成为可能。此外，已经证明在实现我们的数的算术运算：加、减、乘及除时，这种十进制是十分方便的。

§6.2 其它的记数法

世界上各个民族用各种各样的记数法来组织他们的数，关于这些我们有大量的资料。但是，至于这些记数法是为什么和如何创造出来的，则绝大多数都已遗忘于人类的模糊不清的过去了。谁都不怀疑，广为采用的按十来把数分组，是由于人类利用他们的手指来计数这样的事实。相当奇怪的是，很少有用一只手的手指来计数，五进位记数法十分罕见。在另一方面，二十进位制的例子是十分普遍的，容易想到这一定是由于把脚趾也一起用来计数的缘故。马雅人的计数方法可能是这些二十进位制中最为著名的一种，直到不多

几个世纪之前，它们在欧洲仍是十分普遍的使用。在法国，从80到100的二十进位计数是大家熟悉的，例如

80 = quatre-vingts,

90 = quatre-vingt-dix,

91 = quatre-vingt-onze

等等。

至今仍在丹麦人中盛行的计数方法，可能是我们所较为不熟悉的。这种从前在日耳曼民族中很普遍应用的记数法是如此古怪，所以我们不得不稍为说得详细一点。当我们按20来计数时，很自然地利用这样的说法：

tredsindstyve = 三乘二十，

firsindstyve = 四乘二十，

femsindstyve = 五乘二十。

但是，这种记数法由于下面的约定变得更为复杂了。这种约定是：每当我们数到一定个数的20，然后再多10时，我们就要把这个数说成是在下一个二十取一半，例如

90 = halvfemsindstyve

= 在第五个二十上取一半。

为了完善这种记数法，丹麦人利用了在这些十之前先说出个位数的原则，使得一个数的构成如下：

93 = treoghalv femsindstyve

= 三及第五个二十的一半。

显然，象我们这样的到处充满着数的文明社会中，这种记数法肯定是要受到诅咒的。一些计数方法的一个特别令人讨厌的方面，就是要在这些十之前先给出个位数。直到十八世纪以前，这在英国是很流行的，人们把二十三说成三及二十。几年前，挪威议会通过法律在学校教学和所有官方文件

中废除了这种记数法。但它仍然盛行于德国，而且是引起无数差错的原因，例如，在自动电话中。

古老的巴比伦的六十进位制(基数60)，为自古至今的天文学家所利用，虽然它已显得不太方便。在角度和时间的分与秒的计算中，我们仍然使用这种进位制。我们并不知道为什么巴比伦人要引进如此大的基数。人们猜测，它可能来源于两个具有不同基数的进位制的结合。比如说，10和12的最小公倍数是60。

现在我们可以来说几句有关使用各种进位制的数学问题的话了。以 b 为基，整数 N 可写为

$$N = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_2 b^2 + c_1 b + c_0. \quad (6.2.1)$$

这与式(6.1.2)完全一样，所不同的只是代替式(6.1.3)中的数值，这里系数 c_i 可取以下各值：

$$c_i = 0,\ 1,\ \cdots,\ b-1. \quad (6.2.2)$$

为了简单起见，与式(6.1.1)相对应，我们可把式(6.2.1)中的数 N 缩写为

$$(c_n, c_{n-1}, \cdots, c_2, c_1, c_0)_b, \quad (6.2.3)$$

但必需在式(6.2.3)中标出基数 b，以免混淆。

例　在60进位制中有

$$(3,11,43)_{60} = 3 \cdot 60^2 + 11 \cdot 60 + 43 = 11503.$$

在基数 $b=4$ 的进位制中，

$$(3,2,0,1)_4 = 3 \cdot 4^3 + 2 \cdot 4^2 + 0 \cdot 4 + 1 = 225.$$

一般地，当我们用基数为 b 的进位制给出一个数（如式(6.2.1))时，可以用如下的方法，在通常的十进制中求得这个数：先算出 b 的各次方幂的值，再乘上相应的数字(系数)，最后把这些数加起来。这正如我们在上面的例子中所做的一样。

下面我们来讨论相反的问题：给出一个数 N，我们要用基数 b 来表示它。这只要重复地除以 b 就能做到。观察公式(6.2.1)，我们可把它写为

$$N=(c_n b^{n-1}+\cdots+c_2 b+c_1)b+c_0.$$

因为 c_0 小于 b，所以它是 b 除N时所得的余数。我们可把它写为

$$N=q_1 b+c_0,\quad q_1=c_n b^{n-1}+\cdots+c_2 b+c_1.$$

用同样的方法可以证明，用 b 去除 q_1 就得到 c_1，依此类推。这样，通过一系列的除以 b 的除法，我们就求出了所有的系数 c_i：

$$\begin{aligned} N&=q_1 b+c_0,\\ q_1&=q_2 b+c_1,\\ &\cdots\cdots\cdots\\ q_{n-1}&=q_n b+c_{n-1},\\ q_n&=0\cdot b+c_n. \end{aligned}$$

正如所指出的，这种除法一直做到 $q_n<b$，$q_{n+1}=0$ 时为止。通过下面的两个例子可以把这一方法弄清楚。

例 1 用基数 3 来表示数101。同上面那样，我们来做除以 3 的除法，得到

$$\begin{aligned} 101&=33\cdot 3+2,\\ 33&=11\cdot 3+0,\\ 11&=\ \ 3\cdot 3+2,\\ 3&=\ \ 1\cdot 3+0,\\ 1&=\ \ 0\cdot 3+1. \end{aligned}$$

这就给出

$$101=(1,0,2,0,2)_3.$$

例 2 用基数12来表示1970。这里做除以12的除法，得

到

$$1970 = 164 \cdot 12 + 2,$$
$$164 = 13 \cdot 12 + 8,$$
$$13 = 1 \cdot 12 + 1,$$
$$1 = 0 \cdot 12 + 1.$$

因此

$$1970 = (1,1,8,2)_{12}.$$

习　　题

1. 在十进制中表示数

$$(1,2,3,4)_5; \quad (1,1,1,1,1,1)_3.$$

2. 用基数 $b = 2, 6, 17$ 来表示数362；1969；10000.

§6.3　记数法的比较

美国十二进制协会公开申明，应以12为基数的进位制来代替我们的十进制，它认为这是更为有效而方便的.倡议者们指出：有这样一种进位制是有好处的，它的基数可被整数2，3，4，6整除，因而使得经常重复出现的以这些数为除数的除法做起来较为简单。根据这种理由就将导致60进位制的采用，因为基数60可被这样一些小的整数：

2，3，4，5，6，10，12，15，20，30

所整除。

许多东西至今仍以一打（十二个）和一箩（即十二打）来计算，所以有一种十二进位制肯定是方便的。不过，这样一来，我们就应该去引进十二个新的符号来作为十二进制的数字，而且用它们来作运算时，应该象十进制一样漂亮。一些热心的人曾说，只要引进两个新符号来代表10和11就够

了。但这是行不通的，因为在一些情形下，我们将看不出一个给定的数的变化周期，例如，我们不能确定325究竟是表示

$$3\cdot10^2+2\cdot10+5=325,$$

还是表示

$$3\cdot12^2+2\cdot12+5=461.$$

一个数从一种进位制变到由另一种进位制表示时，它的数字的位数将如何变化呢？为了得到关于这种变化的一个粗略的概念，我们来考虑十进制中的数

$$10^n-1=\overbrace{99\cdots9}^{n}=N, \qquad (6.3.1)$$

这是具有 n 位数字的最大的数。为了求出以基数 b 来表示时，它所有的数字的位数 m，我们就必须去确定满足

$$b^m>10^n-1\geqslant b^{m-1} \qquad (6.3.2)$$

的整数 m。这条件可写为 $b^m\geqslant10^n>b^{m-1}$。取这三个数的对数，并注意到 $\log10=1$，就推得

$$m\log b\geqslant n>(m-1)\log b.$$

这也可写为

$$m\geqslant\frac{n}{\log b}>m-1, \qquad (6.3.3)$$

所以 m 是第一个不小于

$$\frac{n}{\log b} \qquad (6.3.4)$$

的整数。因此，粗略地说，我们证明了：新的数字的位数 m 可由 $\log b$ 除以 n 来得到。

例 设 n 是一个数，求用十进制表示其数字的位数。对于 $b=2$，我们有 $\log2\approx0.30103$，所以这个数采用二进制表示时，数字的位数近似等于 $3.32n$。当 $b=60$ 时，$\log60\approx$

1.778，所以数字的位数近似等于0.56n，即比十进制中的数字位数的一半多一点。

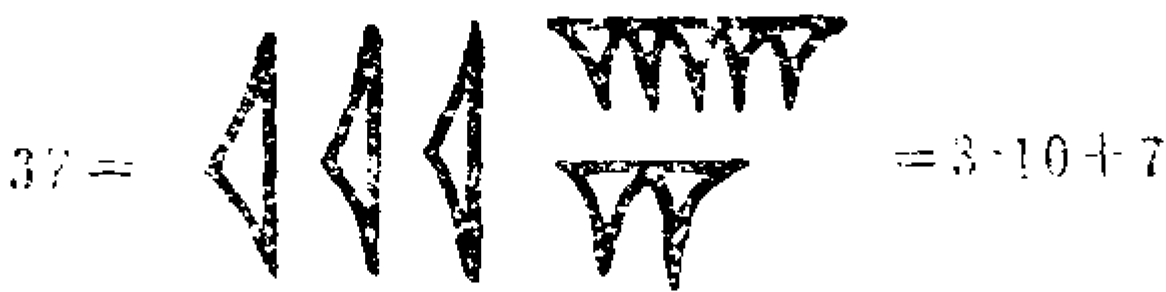


图 6.3.1

显然，用数字位数少的数来进行运算应该是方便的。但另一方面，大的基数有严重的缺点。首先，对这 b 个独立的数字要有各自的名称和符号。但通常对大的 b 并不这样做。例如，在巴比伦的六十进制中，从 1 到60每个个位数是按十个一组来计数的，如图6.3.1中所示。

事实上，它意味着这一进位制已被分解为一些十进位的子进位制。类似的情形也存在于马雅人的20进制中。这里，从 1 到20的数字是以 5 个为一组来计数的，如图6.3.2所示.

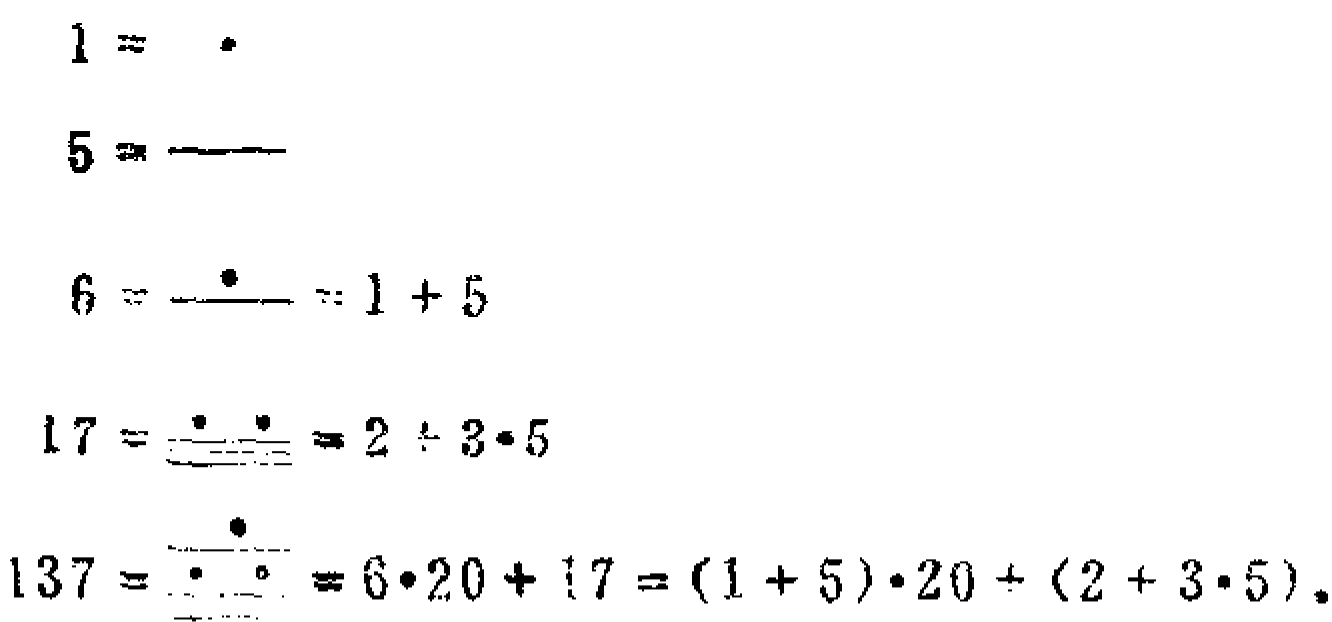


图 6.3.2

其次，更大的困难出现在我们开始按照通常的方式去实行计算的时候。在十进制中，我们做乘法是依赖于我们所熟记的乘法表，即十个数字相互之间的所有的乘积。这张毕达哥拉斯表——正如它在许多国家中所称呼的——在进学校的第一年就被灌输给我们，使它几乎成为我们本能的东西。但这一知识决非如我们所想象的那样显然。从中世纪的算术手稿可清楚地看到，在那时乘法接近于较高级的数学，而长除法确实是一种罕见的技巧。而且，我们还可以举出较近期的

例子来说明这一点。

以日记闻名于世的塞缪尔·佩皮斯（Samuel Pepys），在1662年夏已快三十岁了，他是英国掌管御玺的官员。当时他决定自己独立去核对账目，为此他应该懂得一些数学，至少懂得一些基本的算术。那时，他已经得到了剑桥大学的学士和硕士学位。但是，一个受过优良教育的英国绅士，根本不懂得日常的算账，并不是少见的现象。因为这些事情可以让下面的会计人员去处理。

1662年7月4日，佩皮斯在其日记中写道："不久，我在'罗亚尔·查尔斯'学院的同学库柏先生来了，我打算跟他学数学，而且从今天就开始。他是一位极有才能的人，我想不会有多大问题，我会使他满意的。跟他学了一个小时的算术后（我的第一个愿望是学习乘法表），我们就分别了，次日再见面。"

佩皮斯从早到晚一天又一天的跟他的海员教师拚命地学习那令人生厌的乘法表。例如，他在7月9日写道："一直钻研我的乘法表，直到四点钟。其艰难程度实为我在算术中所从未遇到过的。"以后的几日，他仍同样地学习，直到7月11日他才说自己学会了乘法表："钻研我的乘法表直到四点钟，我现在才差不多可以应用它了。"以后，佩皮斯在他所担任的各种愈来愈重要的职位上，很好地利用了这些新学会的知识。不过，看来他晋升得太快了些，仅在学会了乘法表的二年半之后，他就成为了不列颠科学院——皇家学会的会员。

这种趣闻决不是唯一的。我们这里穿插这一小故事的目的，是在于强调这样一点：在较早的时候，在数学知识的学习中，乘法表并不是很容易的一步。因此，在我们的算术

中，利用小的基数，对心算和机器计算都有不少好处。例如，当基数为$b=3$时，在乘法表

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	$(1,1)_3$

中，仅有一个非显然乘法，即

$$2\cdot 2=4=(1,1)_3.$$

对$b=2$，我们有完全显然的乘法表：

	0	1
0	0	0
1	0	1

习　题

1. 证明：在基数为b的数系中，数字的非显然乘法（即不计乘以0与1的乘法）的个数是

$$\frac{1}{2}(b-1)(b-2).$$

2. 乘法表中，所有的项之和等于多少？对$b=10$验证所得的结果。

§6.4　与记数法有关的一些问题

让我们来讨论几个与记数法有关的问题，这些问题与选择适用于机器计算的基数有某些关系。假设我们与一架普通的台式计算机打交道，它依靠一些互相啮合的数轮来进行运转，在每一个数轮上有10个数字$0,1,\cdots,9$。如果有n个轮子，那么我们就可以表示从1到 …

$$N = \overbrace{99 \cdots 9}^{n} \qquad (6.4.1)$$

（正如式（6.3.1）给出的）的所有的数。现在假定我们要用基数 b 来代替基数10，但仍然要考虑直到N的所有的数。这时，我们一定要有m个轮子，m是满足式（6.3.2）和（6.3.3）的整数。正如式（6.3.4）所指出的：m是不小于

$$\frac{n}{\log b}$$

的第一个整数。因为每个轮子上有 b 个数字，所以，所有轮子上的数字的总的个数近似等于

$$D = n\frac{b}{\log b}. \qquad (6.4.2)$$

现在我们可以问：如何选择基数 b，才能使得所有轮子上的数字的个数为最小？为了求出式（6.4.2）中的数D的最小值，我们只需对各种基数$b=2,3,4,\cdots$来考察函数

$$f(b) = \frac{b}{\log b}. \qquad (6.4.3)$$

利用对数表可得如下的数值：

b	2	3	4	5	6
$f(b)$	6.64	6.29	6.64	7.15	7.71

后面的$f(b)$的值更大，例如，对 $b=10$，正如我们已经指出的有$f(10)=10$。根据这些计算，我们得到如下的结论：

当$b=3$时，计算机中的数字的总数为极小。

我们还可看出，当 $b=2$与 $b=4$时，这总数也大不了多少。因此，在这一方面小的基数是有利的。

让我们来讨论这一问题的一个明显的变形。在一架常常

用来教儿童算数的普通算盘上，有若干根金属细棍，每根棍上有九颗可移动的算盘珠，用以表示数目的各位数字。完全一样，我们可以在纸上画出若干条平行线，并以相应多根火柴来表示数字；或者，如同古代的计算沙盘一样，在地上画出这些直线，用小石子表示数字。

让我们继续来考察算盘。如果它有 n 根棍，每根棍上有 9 颗算盘珠，那末我们也能表出从 1 到由式（6.4.1）所给出的数 N 的所有整数。现在我们提出下面的问题：我们能否取另外的基数 b，使得算盘更小些，即可用更少的算盘珠来进行同样的计算。

对于基数 b，每根棍上的算盘珠个数是 $b-1$。如前一样，为使这算盘具有同样的容量 N，数字的位数或棍的根数必须由式（6.3.4）来确定。这就给出了算盘珠总数的一个渐近公式

$$E=\frac{n}{\log b}\cdot(b-1). \qquad (6.4.4)$$

为了求出何时这个数取可能的最小值，我们必须对各个值 $b=2,3,\cdots$ 来研究函数

$$g(b)=\frac{b-1}{\log b}. \qquad (6.4.5)$$

对小的值 b，$g(b)$ 的值由下表给出：

b	2	3	4	5	6
$g(b)$	3.22	4.19	4.98	5.72	6.43

对较大的值 b，函数值继续增加。所以，我们得出结论：

在一架算盘中，当 $b=2$ 时所需要的算盘珠的总数为最小。

我们可以从另一观点来解释这一结果。现在假定我们用放在直线上的火柴或小石子来表示我们的数的各位数字。这样，在十进制中每条直线上将有 0 到 9 个标记。因此，当我们随机地表出一些数时，在每条直线上所放的火柴的平均数为$4\frac{1}{2}$，所以，随机地把一个 n 位数这样表示时，平均起来就需要$4\frac{1}{2}\cdot n$根火柴。

我们来考虑把这些火柴放在其所在的位置上所需要的时间。为了心中有一个确定的数值，假定每放一根火柴需时一秒。这样，表示一个 n 位数所需要的时间平均起来大概是$4\frac{1}{2}\cdot n$秒。

假定我们把基数变为 b，并要求所能表出的数有同样的容量。这时，每一直线上可能有 0 到 $b-1$ 根火柴，因此它们的平均数为

$$\frac{1}{2}(b-1).$$

正如我们已多次说到的，这时将近似地有

$$\frac{n}{\log b}$$

条直线。我们可得到结论：表示出(十进制中的)一个 n 位数所需的平均时间约为

$$\frac{n}{\log b}\cdot\frac{1}{2}(b-1)=\frac{1}{2}E$$

秒，这里 E 由式(6.4.4)给出。因为当 $b=2$时为极小，所以这里也可断言：

当$b=2$时，表示出一个数所需的平均时间为最小。

习　题

1．设$b>1$，试画出式（6.4.3）中的函数$y=f(b)$及式（6.4.5）中的函数$y=g(b)$的略图。如果你熟悉微分学，那末，就用它来确定这两条曲线的形状。

§6.5　计算机及其记数法

在电子计算机出现之前，十进制在所有的数值计算领域内占有至高无上的地位，而对其它记数法的兴趣，主要是出于历史和文化上的原因。仅有少数的几个孤立的数学问题，用二进制或三进制可以给出最好的表述。在数论书中最为人喜爱的例子之一是所谓筹码游戏。

当计算机以多种形式逐渐发展起来的时候，要设计制造出这样的“硬件”，使得机器尽可能地有效，体积尽可能地小，就变得是最重要的了。这就引起了对各种记数法的深入研究，以确定最合适的一种。出于许多理由（其中一些我们已在前一节中讨论过了），二进制是最佳候选者。事实上，选用它的主要障碍是：我们是在一种不同的遗产——十进制——中成长起来的。但对大多数人来说，只需要经过不多的简单的努力，就可以象对十进制一样的对二进制运用自如，因此，由于要输入计算机的数，通常是以十进制给出的，所以需要一架简单的机械把它们变为二进位数，并在末了把答案仍用十进制来表示，以适应社会上缺少数学训练的人。

当然，用于计算机的二进制与我们上一节所讨论的一样，但所使用的术语有更为专门化的倾向。例如，二进制数字0，1被称为**比特**，这是bits的音译（bits 是英文二进制数字BInary

digiTS 的缩写)。还有，因为在每一个位置上仅出现 0 与 1 这两种可能性，所以人们常常说双态装置。

按照 § 6.2中所阐明的一般规则，我们可以很简单的把一个给定的数用二进制来表示。让我们取 $N=1971$来作为一个例子。重复地用 $b=2$ 除得到：

$$1971=985\cdot2+1,\quad 985=492\cdot2+1,$$
$$492=246\cdot2+0,\quad 246=123\cdot2+0,$$
$$123=61\cdot2+1,\quad 61=30\cdot2+1,$$
$$30=15\cdot2+0,\quad 15=7\cdot2+1,$$
$$7=3\cdot2+1,\quad 3=1\cdot2+1,$$
$$1=0\cdot2+1.$$

因此，

$$1971_{10}=(1,1,1,1,0,1,1,0,0,1,1)_2.$$

前面我们指出过，在二进制中数有较长的表示式，因此，若要稍为看一下就能估计出此数的大小，就变得更困难了。为此，计算机语言常常利用八进制(基数为 8)。这只是二进制的一种简单变形，它可以通过把一个数在二进制中表示的数字按三位数一组分组来得到。我们可以把这看作为基数

$$b=8=2^3$$

的一种记数法，其系数是如下的八个数：

$$0=000,\quad 4=100,$$
$$1=001,\quad 5=101,$$
$$2=010,\quad 6=110,$$
$$3=011,\quad 7=111.$$

我们取上面例子中的数1971来作一解释，在八进制中它变为

$$1971=011;\ 110;\ 110;\ 011=(3;6;6;3)_8.$$

正如我们看到的，这与通常写出一个数的方法没有什么不同。事实上，我们在常用的十进制中，就十分熟悉这种书写方式；在写与读一个大数时，我们常常把数字分为三个一组，例如，

$$N=89\ 747\ 321\ 924。$$

实质上我们可以说，这是数 N 对于基数

$$b=1000=10^3$$

的表示式。

在计算机中，另外一些数的表示法有时是有用的。假如我们希望在适用二进制的机器中，储存一个十进制的数，比如说 $N=2947$。那末，代替把 N 整个地变为二进制的数，我们可以只译出它的各位数字

$$2=0010, \quad 9=1001,$$

$$4=0100, \quad 7=0111,$$

并以

$$N=0010;\ 1001;\ 0100;\ 0111$$

作为 N 存入机器。这种数称为**二进制编码的十进制数**。这一方法有时被称为8421制，因为所有的十进制的数字，可表为以下的二进制单位之和：

$$0=0000, \quad 1=0001, \quad 2=0010,$$

$$2^2=4=0100, \quad 2^3=8=1000。$$

这些二进制编码的十进制数，不适用于任何种类的数值计算。但利用机器的目的，并不总是进行数值计算。同样，任意一个字母及任意其它的符号，都可以指定某一个二进位数与之相对应，这意味着任意一个字或一个句子，都能够作为一个二进位数储存于机器中。所以，如果我们经过专门训练，并有一个同样精通于此的对话者，那末，我们完全可以

利用比特来进行谈话。

习　题

1．求出费马数（§2.3）

$$F_t = 2^{2^t} + 1$$

的二进制表示式。

2．求出偶完全数（§3.4）

$$P = 2^{p-1}(2^p - 1)$$

的二进制表示式。

§6.6　数字游戏

有许多种用数来进行的游戏，其中有一些可追溯到中世纪。它们中的大多数，在数论中具有一些理论上的重要性，说得更恰当一些，它们象幻方一样，属于纵横数谜这一类问题。我们将通过例子来说明其中几个。

一个大学生在其打给家中的电报中，提出了这样的紧急请求①：

```
   S E N D
   M O R E
 ---------
 M O N E Y
```

如果每一个字母表示一个不同的数字，我们可把这一格式看作为两个四位数 SEND 与 MORE的加法，其和为 MONEY．问题是要来确定这些数字可能是什么？因为仅有十个数字，所以在每一个这种问题中，至多能有十个不同的字母。在这

① 请读者自己注意一下这类问题中的英文字的意义，就会发现是很有趣的。——译者

一例子中，有 8 个不同的字母。理想的形式是问题应该有唯一解。

在我们的例子中，必有

$$M = 1,$$

因为 M 是数 $S+M$ 或 $S+M+1$ 中的第一位数字，而 S 与 M 是不大于 9 的数字。这样，S 有两种不同的可能：因为 $S+1$ 或 $S+1+1$ 是一个二位数，所以一定要

$$S=9 \quad 或 \quad S=8.$$

我们首先证明 S 不可能是 8。因为，如果 S 是 8，那末，应该在百位列上有一进位，使得在千位列上的加法得到

$$S+M+1=8+1+1=10.$$

因此，字母 O 应为零，而电文将被理解为

```
  8 E N D
  1 0 R E
---------
1 0 N E Y
```

但是，通过考察百位列可知，十位列上必须有一进位(不然 $E+0=E$，不等于 N)，再因为 $E \leqslant 9$，因此将有

$$E+0+1=10.$$

而这将迫使我们去设 $N=0$，但这是不可能的，因为我们已经有 $O=0$。这就证明了

$$S=9.$$

因而电文可以理解为

```
  9 E N D
  1 0 R E
---------
1 0 N E Y
```

因为 $E \neq N$，所以在百位列上的加法必导致

$$E+1=N,$$

这样就有

$$\begin{array}{cccc} 9 & E & E+1 & D \\ 1 & 0 & R & E \\ \hline 10 & E+1 & E & Y \end{array}$$

在十位列上的加法有两种可能：

$$E+1+R=10+E \quad 或 \quad E+1+R+1=10+E.$$

第一种情形是不可能的，因为这给出 $R=9$，而这与 $S=9$ 相矛盾，在第二种情形，

$$R=8,$$

因而电文可理解为

$$\begin{array}{cccc} 9 & E & E+1 & D \\ 1 & 0 & 8 & E \\ \hline 10 & E+1 & E & Y \end{array}$$

最后，在个位列上的和是

$$D+E=10+Y.$$

对于这三个字母 D,E,Y，仅可在2,3,4,5,6,7 中取值。其中任意两个不同的数之和至多为 13，所以仅有 $Y=2$ 或 $Y=3$ 这两种可能。后者是不可能的，因为这将给出 $D+E=13$，但我们既不可能有 $E=7$，因为这时将有 $N=E+1=8=R$；也不可能有 $D=7$，因为这时将有 $E=6$ 及

$$N=E+1=7=D.$$

这样一来，我们必有 $Y=2$及$D+E=12$，在可选择的数字 2,3,4,5,6,7 中，和为 12 的两个数仅可能是5与7。因为 $E\neq7$，所以就推出 $D=7$，$E=5$。因此我们的问题的唯一解是：

$$\begin{array}{r} 9567 \\ 1085 \\ \hline 10652 \end{array}$$

这一解题过程显然是经过精心考虑的。而实际上在许多情形，求解要容易得多。

习　题

试用我们刚才说明的方法来分析下面的问题。

```
1.  S E N D      2.   S E E      3.  A D A M
    M O R E           S E E            A N D
    G O L D           S E E            E V E
  ---------           Y E S              O N
  M O N E Y         -------                A
                    E A S Y          -------
                                     R A F T

4.  F O R T Y             5.  H O C U S
        T E N                 P O C U S
        T E N               -----------
  -----------               P R E S T O
    S I X T Y
```

如果你有兴趣，自己可以试着提出一些问题。如果你熟悉使用计算机，可试编一些求解这种问题的程序。

第七章 同 余

§7.1 同余的定义

数论有它自己的代数，称为同余理论。普通的代数最初是作为算术运算的一种速记法而发展起来的。类似地，同余是代表数论的基本概念——可除性的符号语言。首先引进同余概念的是高斯。

在转入讨论同余之前，我们先对将要在本章中研究的数作一点说明。在本书一开头说过，我们所研究的是正整数1，2，3，…；在前几章中，我们限于讨论这些数及0。但现在已到了这样一个阶段——把我们所讨论的数的范围扩大到包括全体正负整数是有好处的，即讨论

$$0,\ \pm 1,\ \pm 2,\ \pm 3,\cdots.$$

这样做在任何本质方面都不影响我们前面所引进的概念。但是，当我们以后说到素数、除数(因数)、最大公约数，以及其它类似的概念时，仍然把它们看为正整数。

现在让我们转入同余语言。若 a 与 b 是两个整数，且它们的差 $a-b$ 被 m 整除，那末，我们就用式子

$$a\equiv b \pmod m \qquad (7.1.1)$$

来表示这一关系，并读作

$$a\text{ 同余于 }b\text{，模}m. \qquad (7.1.1)$$

假定除数 m 是正的，称它是这同余式的模。同余式(7.1.1)意味着

$$a-b=mk,\quad k\text{整数}. \qquad (7.1.2)$$

例 1) $23\equiv 8 \pmod 5$，因为$23-8=15=5\cdot 3$。

2) $47\equiv 11 \pmod 9$，因为$47-11=36=9\cdot 4$。

3) $-11\equiv 5 \pmod 8$，因为$-11-5=-16=8(-2)$。

4) $81\equiv 0 \pmod{27}$，因为$81-0=81=27\cdot 3$。

最后一例表明，在一般情形下，我们可以写

$$a\equiv 0 \pmod m$$

来代替说 a 可被 m 整除，因为这式子意味着

$$a-0=a=mk,$$

这里 k 是某一整数。例如，代替说 a 是一个偶数，可以写

$$a\equiv 0 \pmod 2.$$

同样的，可以看出奇数是满足

$$a\equiv 1 \pmod 2$$

的数。这种多少有点奇怪的术语，在数学论文中是十分普通的。

§7.2 同余式的一些性质

我们书写同余式的方式，使我们想起等式，而事实上，同余式和代数等式有一些相同的性质。最简单的是以下三个：

$$a\equiv a \pmod m, \tag{7.2.1}$$

这是 $a-a=0=m\cdot 0$ 的一个推论。

$$a\equiv b \pmod m \quad \text{推出} \quad b\equiv a \pmod m, \tag{7.2.2}$$

这可从 $b-a=-(a-b)=m(-k)$推出。从

$$a\equiv b \pmod m \quad \text{及} \quad b\equiv c \pmod m \tag{7.2.3}$$

可推出

$$a\equiv c \pmod m.$$

因为前两式意味着

$$a-b=mk,\qquad b-c=ml,$$

所以

$$a-c=(a-b)+(b-c)=m(k+l).$$

例 从

$$13\equiv35\ (\text{mod }11),\qquad 35\equiv-9\ (\text{mod }11)$$

可推出

$$13\equiv-9\ (\text{mod }11).$$

我们说过同余式与等式在其性质上相似。事实上，我们可以把等式看作为同余式的一种，即模为0的同余式。这只要定义

$$a\equiv b\ (\text{mod }0)$$

为

$$a-b=0\cdot k=0\quad 或\quad a=b.$$

你几乎永远不会在数学文献中遇到把等式写为这种形式的同余式。但是，有时偶尔使用另外一种看来是十分显然的同余式。当模 $m=1$ 时，对任意一对整数 a 与 b 有

$$a\equiv b\ (\text{mod }1),\tag{7.2.4}$$

因为这意味着

$$a-b=1\cdot k=k\tag{7.2.5}$$

是一个整数。但让我们现在，也仅在现在，假定 a 与 b 是任意实数，而不必是整数。那末，它们同余(mod 1)意味着它们之差是整数，即这两个数有同样的分数部分(或小数部分，如果它们用十进制来表示)。

例

$$8\frac{1}{3}\equiv1\frac{1}{3}\ (\text{mod }1)$$

或

$$8.333\cdots\equiv 1.333\cdots \pmod 1.$$

让我们回到通常的整数同余式的性质上来；从现在起我们总假定模是一个整数 $m\geqslant 2$。

我们可从原点开始，在两个方向上，把数轴分为长度为 m 的区间，如图 7.2.1 所示。这样一来，每一个整数 a，正的或负的，必落入这些区间中的一个或恰好在一个分划线上，所以我们可写

$$a=km+r, \tag{7.2.6}$$

这里 k 是某个整数，r 是数

$$0,\ 1,\ 2,\ \cdots,m-1 \tag{7.2.7}$$

中的一个。这是 § 4.3 中正整数除法的一个明显的推广。同样的，这里我们也把(7.2.6)中的 r 称为 a 被 m 去除的余数，或称为 a 的余数(mod m)。

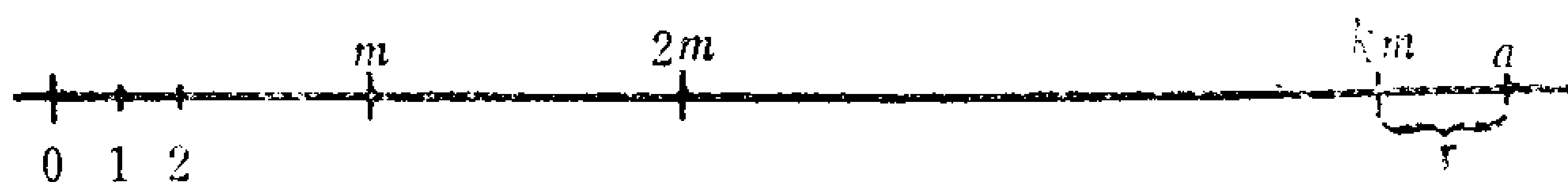


图 7.2.1

例

1) $a=11$，$m=7$，$11=7\cdot 1+4$。

2) $a=-11$，$m=7$，$-11=7(-2)+3$。

这种除法(7.2.6)也可被写为同余式的形式

$$a\equiv r \pmod m, \tag{7.2.8}$$

所以，每一个数同余于它的余数(mod m)。在上面的例子中有

$$11\equiv 4 \pmod 7,\qquad -11\equiv 3 \pmod 7.$$

在式(7.2.7)中没有两个余数同余(mod m)，因为它们中的任意两个数之差小于 m。所以，两个对模 m 不同余的数，一定有不同的余数(mod m)。所以，我们得到结论：

当且仅当 a 与 b 被 m 去除有相同的余数时，同余式 $a \equiv b \pmod{m}$ 才成立。

还有另一种表述这种同余关系的方式。暂时设 a 与 b 是正整数。在§6.2关于记数法的讨论中，我们看到当 a 以基数 m 来表示时，

$$a = (a_n, \cdots, a_1, a_0)_m,$$

其末位数字 a_0 就是 a 被 m 除的余数。如果用这种看法来重新解释同余关系，我们就可以说：

当且仅当(正)整数 a 与 b 以基数 m 来表示有相同的末位数时，同余式 $a \equiv b \pmod{m}$ 才成立。

例 $$37 \equiv 87 \pmod{10},$$

因为这两个数在十进制中，有相同的末位数。

习　题

求余数

$-37 \pmod{7}$；　$-111 \pmod{11}$；　$-365 \pmod{30}$。

§7.3　同余式的代数

我们记得在代数中，等式可以相加，相减和相乘。完全同样的规则对同余式也成立。假设我们有同余式

$$a \equiv b \pmod{m}, \qquad c \equiv d \pmod{m}. \tag{7.3.1}$$

根据定义这意味着

$$a = b + mk, \qquad c = d + ml, \tag{7.3.2}$$

其中 k 与 l 是整数。把(7.3.2)式中的这两个等式相加，得到

$$a + c = b + d + m(k + l),$$

而这可写为

$$a + c \equiv b + d \pmod{m}, \tag{7.3.3}$$

换句话说，两个同余式可以相加。同样可以证明：可从一个同余式中减去另一个同余式，即

$$a-c \equiv b-d \pmod{m}. \tag{7.3.4}$$

例

$$11 \equiv -5 \pmod{8} \quad 与 \quad 7 \equiv -9 \pmod{8}. \tag{7.3.5}$$

相加得

$$18 \equiv -14 \pmod{8},$$

相减得

$$4 \equiv 4 \pmod{8}.$$

我们也可以把两个同余式相乘。由式(7.3.1)与(7.3.2)相乘得

$$ac = bd + m(kd + bl + mkl),$$

所以

$$ac \equiv bd \pmod{m}. \tag{7.3.6}$$

例 当式(7.3.5)中的两个同余式相乘时，得到

$$77 \equiv 45 \pmod{8}.$$

同余式

$$a \equiv b \pmod{m}$$

能乘以任一整数 c，给出

$$ac \equiv bc \pmod{m}. \tag{7.3.7}$$

这可以看作乘法(7.3.6)当 $c=d$ 时的一个特例。

例 当式(7.3.5)中的第一个同余式乘以3时，得到

$$33 \equiv -15 \pmod{8}.$$

一个很自然的问题是：什么时候我们可以在同余式(7.3.7)中约去公因数 c，并得到一个正确的同余式

$$a \equiv b \pmod{m}.$$

在这一点上，同余式不同于等式。例如，我们有

$$22 \equiv -2 \pmod 8,$$

但约去 2 后就给出$11 \equiv -1 \pmod 8$，而这是不正确的。

有一种重要的情形，相约是允许的。

若 $ac \equiv bc \pmod m$，那末，当 m 与 c 互素时，就有 $a \equiv b \pmod m$。

证 第一个同余式意味着

$$ac - bc = (a-b)c = mk.$$

若$(m,c)=1$，则根据§4.2(第42页）中所证明的除法规则，可推出 $a-b$ 被 m 整除。

例 在同余式

$$4 \equiv 48 \pmod{11}$$

中，我们可以约去因数 4，因为$(11,4)=1$。这给出

$$1 \equiv 12 \pmod{11}.$$

习　题

对上面所说的各种同余式的运算规则，给出你自己的一些例子。

§7.4　同余式的方幂

再假设我们有同余式

$$a \equiv b \pmod m.$$

正如我们刚才所看到的，可以把这同余式与它自己相乘，得到

$$a^2 \equiv b^2 \pmod m.$$

一般地，对任意正整数 n，同余式可以自乘足够多次，得到

$$a^n \equiv b^n \pmod m.$$

例 从

$$8 \equiv -3 \pmod{11},$$

取平方得到

$$64 \equiv 9 \pmod{11},$$

取三次方得到

$$512 \equiv -27 \pmod{11}.$$

许多关于同余式的结果与求一个数的高次幂的余数有关。让我们来指出如何处理这一问题。例如，假设要求余数

$$3^{89} \pmod 7.$$

解这一问题的一个方法是重复地进行平方。我们得到

$$9 = 3^2 \equiv 2 \pmod 7,$$

$$3^4 \equiv 4,$$

$$3^8 \equiv 16 \equiv 2,$$

$$3^{16} \equiv 4,$$

$$3^{32} \equiv 16 \equiv 2,$$

$$3^{64} \equiv 4 \pmod 7.$$

因为

$$89 = 64 + 16 + 8 + 1 = 2^6 + 2^4 + 2^3 + 1,$$

由此推出

$$3^{89} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3 \equiv 4 \cdot 4 \cdot 2 \cdot 3 \equiv 5 \pmod 7.$$

因而这一余数(mod 7)是 5；换句话说，根据我们在§7.2中所说的可以推出：在基数为 7 的记数法中，3^{89} 的末位数字是 5。

事实上，为了求得这个余数，我们所做的事情就是把指数用二进制来表示

$$89 = 2^6 + 2^4 + 2^3 + 1 = (1,0,1,1,0,0,1)_2.$$

通过不断的平方，可求出该数的各个二进幂

1，2，4，8，16，32，64

的余数(mod 7)。这个方法总可以用来去求高次幂的余数。

但是，通过巧妙的观察能发现，在一些特殊情形下常常可以更简单地来处理。例如，在上面的情形中我们注意到有

$$3^3 \equiv -1 \pmod 7,$$

$$3^6 \equiv 1 \pmod 7,$$

所以我们得到

$$3^{84} = (3^6)^{14} \equiv 1 \pmod 7.$$

因此，同前面一样有

$$3^{89} = 3^{84} \cdot 3^3 \cdot 3^2 \equiv 1 \cdot (-1) \cdot 2 = -2 \equiv 5 \pmod 7.$$

作为另一个说明，我们可来考虑在§2.3中引进的费马数

$$F_t = 2^{2^t} + 1.$$

开头几个数是

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17,$$

$$F_3 = 257, \quad F_4 = 65537.$$

这看起来暗示着可能有以下的结论：

除了 F_0 和 F_1 外，所有的以十进制表示的费马数均以数字 7 结尾。

让我们利用同余式来证明，情形正是这样。显然，这如同说

$$2^{2^t}, \qquad t = 2, 3, \cdots$$

均以数字 6 结尾是一样的。我们用归纳法来证明这一点。注意到

$$2^{2^2} = 16 \quad \equiv 6 \pmod{10},$$

$$2^{2^3} = 256 \quad \equiv 6 \pmod{10},$$

$$2^{2^4} = 65536 \equiv 6 \pmod{10}.$$

一般地，若平方 2^{2^k} 就得到

$$(2^{2^k})^2 = 2^{2\cdot 2^k} = 2^{2^{k+1}}.$$

假设对某个 t 有

$$2^{2^t} \equiv 6 \pmod{10},$$

那末，平方这一同余式就得到

$$2^{2^{t+1}} \equiv 36 \equiv 6 \pmod{10},$$

这正是所要证明的。

§7.5 费马同余式

我们记得代数学中的二项式定律

$$\left.\begin{aligned} x+y &= x+y, \\ (x+y)^2 &= x^2+2xy+y^2, \\ (x+y)^3 &= x^3+3x^2y+3xy^2+y^3, \\ (x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4, \end{aligned}\right\} \quad (7.5.1)$$

以及一般地，

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + y^p. \quad (7.5.2)$$

这里，第一项和最后一项的系数是 1，中间的二项式系数是

$$\left.\begin{aligned} &\binom{p}{1} = \frac{p}{1}, \quad \binom{p}{2} = \frac{p(p-1)}{1\cdot 2}, \\ &\binom{p}{3} = \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}, \quad \cdots, \end{aligned}\right\} \quad (7.5.3)$$

以及一般地

$$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{1\cdot 2\cdot \cdots \cdot r}, \quad (7.5.4)$$

$$r = 1, 2, \cdots, p-1.$$

正如式(7.5.1)中所指出的，这些系数是通过逐次乘以 $x+y$ 而得到的，所以显然它们是整数。

从现在起假定 p 为素数。为了把式(7.5.4)所给出的这些整数写为整数的形式，我们必须约去在分母

$$1\cdot 2\cdot\cdots\cdot r$$

与分子

$$p(p-1)\cdots(p-r+1)$$

中的公因数。但分母不包含素因数 p，所以相约以后，p 仍然出现在分子中。这样，我们就证明了：

若 p 为素数，那末在式(7.5.2)中的所有的二项式系数(除了第一项和最后一项外)均可被 p 整除。

现设式(7.5.2)中的 x 与 y 是整数。如果我们把公式(7.5.2)看作为一个同余式(mod p)，那末，可以得到

对整数 x 与 y，及任意的素数 p，有

$$(x+y)^p\equiv x^p+y^p \pmod p. \qquad (7.5.5)$$

让我们取 $p=5$ 作为一个例子，有

$$(x+y)^5=x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5.$$

因为中间所有的系数均可被 5 整除，相应于式(7.5.5)，我们得到

$$(x+y)^5\equiv x^5+y^5 \pmod 5.$$

从同余式(7.5.5)我们可以得到一些重要的推论。首先，让我们把它应用于 $x=y=1$ 的情形，这就给出

$$2^p=(1+1)^p\equiv 1^p+1^p=2 \pmod p.$$

下一步我们取 $x=2$, $y=1$，得到

$$3^p=(2+1)^p\equiv 2^p+1^p,$$

然后，我们利用前面的结果 $2^p\equiv 2 \pmod p$ 得到

$$2^p+1^p\equiv 2+1\equiv 3 \pmod p,\text{ 所以 } 3^p\equiv 3 \pmod p.$$

再其次，对 $x=3$，$y=1$，我们可得到

$$4^p \equiv 4 \pmod p。$$

利用这一方法，就可以依次地证明对所有的值

$$a=0,\ 1,\ \cdots,\ p-1 \qquad (7.5.6)$$

有 $a^p \equiv a \pmod p$ 成立。对于特殊情形 $a=0$ 与 $a=1$，这个同余式是显然成立的。因为每一个数和式(7.5.6)中的某一个数同余(mod p)，所以我们证明了：

对任意的整数 a 和任意的素数 p，有

$$a^p \equiv a \pmod p。 \qquad (7.5.7)$$

这一同余定律通常称为**费马定理**，一些作者为了把它和我们在§5.3中提到的费马大定理或费马猜想相区别而称之为**费马小定理**。

例 对 $p=13$ 与 $a=2$，我们可求得 $13=8+4+1$，所以有 $2^{13}=2^{8+4+1}=2^8\cdot2^4\cdot2^1$。因为

$$2^4=16\equiv3 \pmod{13}, \qquad 2^8\equiv9 \pmod{13},$$

故得 $$2^{13}=2^8\cdot2^4\cdot2^1\equiv9\cdot3\cdot2\equiv2 \pmod{13},$$

这正是费马同余式所给出的。

根据在§7.3结束时所讲的同余式的消去律，当 a 与模 p 互素时，我们可以在费马同余式(7.5.7)的两边消去公因数 a。这就给出了下面的结果：

若 a 是一个不被素数 p 整除的整数，那末

$$a^{p-1} \equiv 1 \pmod p。 \qquad (7.5.8)$$

这一结果也称为**费马定理**。

例 当 $a=7$，$p=19$ 时，我们得到

$$7^2=49\equiv11 \pmod{19}, \qquad 7^4\equiv121\equiv7 \pmod{19},$$

$$7^8\equiv49\equiv11 \pmod{19}, \qquad 7^{16}\equiv121\equiv7 \pmod{19},$$

而这就给出

Rechnung auff
der Linien vnnd Federn /
Auff allerley Handtierung /
Gemacht durch
Adam Riesen.



Auffs new mit fleis durchlesen /
vnd zu recht bracht.

Gedruckt zu Magdeburgk / In ver=
legung Johan Francken.

$$a^{p-1}=7^{18}=7^{16}\cdot 7^2\equiv 7\cdot 11\equiv 1 \pmod{19},$$

这正是费马同余式(7.5.8)所要求的。

作为费马同余式(7.5.8)的一个应用，我们回到第五章所讨论的毕达哥拉斯三角形上来，证明以下的结论：

一个毕达哥拉斯三角形的边长的乘积可被60整除。

证 显然，只要对本原三角形来证明就足够了。根据公式(5.2.7)，这乘积是

$$P=2mn(m^2-n^2)(m^2+n^2)=2mn(m^4-n^4).$$

当且仅当数 P 被 4，3 及 5 整除时，它才能被60整除。因为数 m 与 n 中有一个是偶的，所以$2mn$ 可被 4 整除。当数 m 与 n 中至少有一个被 3 整除时，P 被 3 整除。但若 m 和 n 均不能被 3 整除时，P 亦被 3 整除，这是因为根据式(7.5.8)，从$(m,3)=1$及$(n,3)=1$可推出 $m^2\equiv 1 \pmod 3$及 $n^2\equiv 1 \pmod 3$，所以

$$m^2-n^2\equiv 1-1\equiv 0 \pmod 3.$$

类似地可证明 P 被 5 整除。若 m 或 n 被 5 整除，那末这是显然的。如果它们均不被 5 所整除，那末再根据费马同余式(7.5.8)，我们有

$$m^4-n^4\equiv 1-1\equiv 0 \pmod 5.$$

第八章　同余式的一些应用

§8.1　计算的检查

正如我们已经提到的，同余理论的创造者是德国数学家高斯。他关于数论的名著《算术研究》① 出版于1801年，当时他24岁。这本书的前几章讨论同余理论，你现在已经学了足够的同余式的知识，能够去读懂高斯的原著。

但我们应该提到，在高斯的时代之前数世纪，已经有了关于同余理论的一些形迹，其中一些是出现在古代关于算术计算的检查方法之中。这些检查方法构成了文艺复兴时期算术数学的一个主要部分。它们中的某一些方法至今仍在应用。而关于它们的起源，我们所知道的仅仅是它们可能来源于古代。

我们虽然不知道这些方法开始是怎样被引进的。但我们来指出一个看来似乎有些道理的，可能是发现它们的说法，让我们回到计算板的时代。假定用十进制表示数。在这样一个板上，需要作计算的数的每一位数字将用筹码或小石子或小棍来标出，每一组筹码根据它所在的位置标出了 1 的个数，10的个数，100的个数，等等。在十进制中，一个数

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$
$$= (a_n, a_{n-1}, \cdots, a_2, a_1, a_0)_{10} \qquad (8.1.1)$$

将总共需要

$$S_N = a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \qquad (8.1.2)$$

---

① 这一经典著作的英译本最近已由耶鲁大学出版社出版.

根筹码。这个数我们称之为N的数字和。

现在假定我们想在计算板上去做一个简单的运算，即把两个数N和M相加。我们把这第二个数

$$M=(b_m, b_{m-1}, \cdots, b_2, b_1, b_0)_{10},$$

也在同样的那些列上用另外的

$$S_M=b_m+b_{m-1}+\cdots+b_2+b_1+b_0$$

根筹码在板上标出。现在在某些列上可以有多于 9 根筹码。求出$M+N$的运算是这样进行的：把一列上的10根筹码用它的下一列上的 1 根筹码来代替，并继续这样做下去，直到不再有这样的化简为止。由于在每一步都用 1 根筹码去代替10根筹码，所以在板上净少了 9 根。因而，如果这一加法做得正确，那末留在板上的筹码的个数必须满足

$$S_{N+M}\equiv S_N+S_M \pmod 9, \qquad (8.1.3)$$

即仍在板上的筹码数和原来的筹码的总数之差一定是 9 的倍数。对这种检查方法（8.1.3），我们至今仍然用它古老的名称：弃九法。

在发现了这一方法之后，马上就能看出它也可应用于几个数相加，应用于减法及乘法。对于乘法，类似于式（8.1.3），我们有

$$S_M\cdot S_N\equiv S_{MN} \pmod 9). \qquad (8.1.4)$$

利用同余式可以很容易地从理论上来证明这些方法的正确性。显然有

$$1\equiv 1, \quad 10\equiv 1, \quad 10^2\equiv 1, \quad 10^3\equiv 1, \quad \cdots \pmod 9), \qquad (8.1.5)$$

所以从式（8.1.1）和（8.1.2）得到

$$N\equiv S_N \pmod 9). \qquad (8.1.6)$$

因此，根据我们在§7.3中所证明的同余式的性质，显然有

$$S_N \pm S_M \equiv N \pm M \equiv S_{N \pm M} \pmod 9,$$
$$S_N \cdot S_M \equiv N \cdot M \equiv S_{N \cdot M} \pmod 9.$$

弃九法最经常地是用于乘法。我们来看一个例子。取数

$$M = 3119, \qquad N = 3724 \qquad (8.1.7)$$

及乘积

$$M \cdot N = 11614156.$$

这个计算是不正确的。因为若是这样，就将有

$$M \equiv S_M \equiv 3 + 1 + 1 + 9 \equiv 5 \pmod 9,$$
$$N \equiv S_N \equiv 3 + 7 + 2 + 4 \equiv 7 \pmod 9,$$

及

$$MN \equiv S_{MN} \equiv 1 + 1 + 6 + 1 + 4 + 1 + 5 + 6 \equiv 7 \pmod 9.$$

但

$$5 \cdot 7 = 35 \equiv 8 \not\equiv 7 \pmod 9.$$

事实上，这乘积应为

$$M \cdot N = 11615156.$$

在中世纪的学校中，是严格地要求学生把这种检查也包括在他们的练习之中的。所以，在这些年代的手稿中，人们可发现一个附加的十字交叉图。在我们的例子(8.1.7)中，这图有(图8.1.1)的形式。图中两侧的数字5与7表示M与N的余数(mod 9)，而上面的数字8是算得的乘积$M \cdot N$的余数(mod 9)。这一结果应该用在下面的余数的乘积来检查，这里是

$$5 \cdot 7 = 35 \equiv 8 \pmod 9.$$

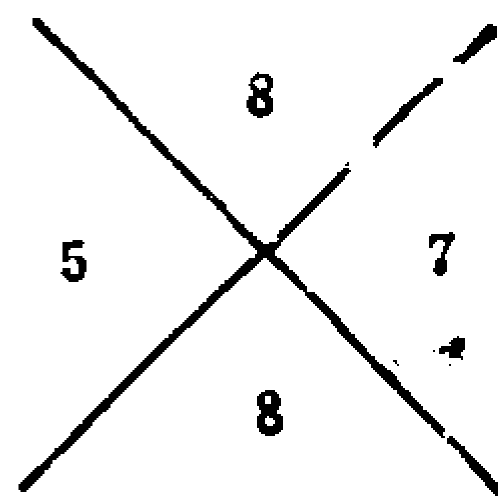


图 8.1.1

这些十字交叉检查十分普遍地出现在早期出版的算术教科书中。例如，在十七到十八世纪

的英国教科书中。当然，这种情形是可能出现的：在一个计算中含有不能由这种弃九法检查出来的错误。但我们知道，这种错误是所谓“模 9 的误差”。

显然，对其它的基数也可以利用类似的检查方法。设基数为 b，对于一个数

$$M = m_n b^n + m_{n-1} b^{n-1} + \cdots + m_2 b^2 + m_1 b + m_0,$$

如同在式(8.1.5)中一样，有

$$1 \equiv 1, \quad b \equiv 1, \quad b^2 \equiv 1, \quad \cdots \pmod{b-1},$$

所以如前一样可得

$$M \equiv S_M = m_n + m_{n-1} + \cdots + m_2 + m_1 + m_0 \pmod{b-1},$$

因此，检查的方法是一样的。

这种看来是十分显然的观察，甚至在通常的十进制中也有应用。在§7.5中我们提到，如果我们以三位数一组来分一个十进位数的数字，那末这种分组可被看作是这个数对于基数

$$b = 10^3 = 1000$$

的表示式。类似地，如果我们把数字按两两分组，那末这就相应于对基数

$$b = 10^2 = 100$$

的表示式。再取数3119及3724来作为例子，把它们写为

$$M = 31\ \ 19, \qquad N = 37\ \ 24,$$

$$M \cdot N = 11\ \ 61\ \ 51\ \ 56,$$

我们得到

$$M \equiv 31 + 19 = 50 \pmod{99},$$

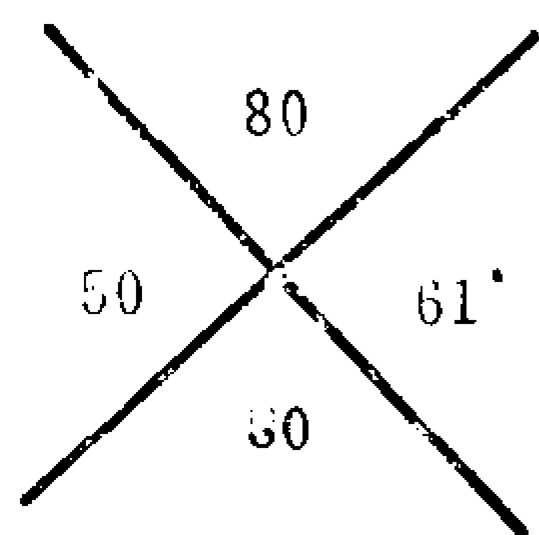
$$N \equiv 37 + 24 \equiv 61 \pmod{99},$$

$$M \cdot N \equiv 11 + 61 + 51 + 56 = 179 \equiv 80 \pmod{99}.$$

因为有

$$50\cdot 61\equiv 80 \pmod{99},$$

所以右图是这里的十字交叉检查图。这种检查方法要比弃九法更加有效，因为这里的模比较大，所以答数是正确的可能性也比较大。换句话说，出现一个“模99的误差”的可能性，比出现一个“模 9 的误差”的可能性理应要小些。



§8.2 日期的星期数①

天文学和年代学中与周期性有关的许多问题可以用数论的概念来陈述。我们这里将只给出一个例子：确定一个给定的日期的星期数。这些星期数本身是以周期 7 重复，所以代替常用的名称我们可以给每一个星期数以一个数目②：

星期日 = 0，　星期一 = 1，

星期二 = 2，　星期三 = 3，

星期四 = 4，　星期五 = 5，

星期六 = 6。

当我们这样做以后，每一个整数就对应于一个星期数，即它的余数(mod 7) 所确定的那一个星期数。

假如我们有这样一个可喜的情况：一年中的天数可被 7 整除，那末，所有的日期(不计年份)在每一年中总有同样的星期数，这样，日历的编制将变得简单，而日历出版商的生意就将大大减少。然而，一年的天数是

$$365\equiv 1 \pmod{7},$$

而闰年的天数为

① 我们把星期日，星期一，…等，称为星期数．——译者

② 我们同样把这些数目也称为星期数．——译者

$$366 \equiv 2 \pmod 7) .$$

这表明对非闰年来说，一个给定日期(不计年份)的星期数W将在下一年增加1。例如，某一年的一月一日是星期日($W=0$)，那末在下一年将是星期一($W=1$)。这并不复杂。但是，这种简单的规律当遇到闰年时就被破坏了。闰年每四年出现一次，而这时星期数将增加2；此外，我们的另一困难是，在闰年所加的一天既不是在一年的开头，也不是在一年的末尾，而是在一年之中的二月廿九日。这一情形使得我们作出如下的约定：把三月算作第一个月，四月算作第二个月等等，而把一月算作上一年的第十一个月，二月算作上一年的第十二个月。这一约定对下面给出W的一般公式是有好处的。

但我们还有困难。在根据尤利乌斯·恺撒的法令所实行的恺撒历中，按照闰年的规律，把一年恰好规定有$365\frac{1}{4}$天。然而，这是不十分正确的，因为天文年实际上有

365.2422天。

这一小误差逐渐引起了季节和日历关系之间不应有的大变化。例如，在十六世纪，春分是三月十一日，而不是原来的三月廿一日。

为了纠正这一状况，教皇格里哥利十三在几经斟酌之后，于1582年在天主教国家实行了他的历法改革。先把十月五日(星期五)这一天改为十月十五日(星期五)，用这样的办法在这一年中减少了十天。进而，为了保持日历与季节的协调一致，采用了下面的格里哥利闰年规则：

世纪数不能被4整除的世纪年①

① 世纪数指下面式(8.2.1)中的数C，这同我们通常的十六世纪、十七世纪等的说法不一致。一个世纪的第一年(即$Y=0$)称为世纪年。——译者

1700， 1800， 1900， 2100， 2200， 2300， …

不是闰年。而其余的世纪年

1600， 2000， 2400， …

仍作为闰年。这样，我们得到了一年的正确长度的一个很好的近似。但现在看来这又显得有点太短了。所以同格里哥利规则不同，已经提出把4000年，8000年，……不作为闰年。因为这是一个仍然沒有解决，但又与最近的将来沒有关系的问题，所以在我们的公式中可以不考虑这一点。

现在假定我们有一个给定的日期：第N年m月d日，这里，年份数

$$N = C \cdot 100 + Y, \qquad (8.2.1)$$

C是世纪数，Y是在这一个世纪中的年份数，月份数m按上面的规定计算。那末可以证明：这一日期的星期数可由同余式

$$W \equiv d + \left[\frac{1}{5}(13m-1)\right] + Y + \left[\frac{1}{4}Y\right] + \left[\frac{1}{4}C\right] - 2C \pmod 7 \qquad (8.2.2)$$

来确定。由§4.3可知，公式中出现的方括号表示不超过这个数的最大整数。

例 珍珠港日，1941年12月7日。这里

$$C = 19, \quad Y = 41, \quad m = 10, \quad d = 7,$$

所以

$$W \equiv 7 + 25 + 41 + 10 + 4 - 38 \equiv 0 \pmod 7),$$

即这一天是星期日。

例 2000年1月1日是星期几？这里

$$C = 19, \quad Y = 99, \quad m = 11, \quad d = 1,$$

以及

$$W \equiv 1+28+1+3+4-38 \equiv 6 \pmod 7),$$

所以，下一个世纪的第一天将是星期六。

必须注意到：在格里哥利历采用之前，不能应用这公式来计算星期数。英国和它的殖民地，是在1752年采用格里哥利历的。当时是把9月3日改为新历9月14日，使得这一年减少了十一天。

你或许希望详详细细的知道这个公式是如何建立起来的。如果不想知道，则可略去这一节的以下部分。我们把这一分析分为两部分。

首先，让我们来确定任意一年N（由式(8.2.1)给出）中的3月1日的星期数。我们任意取定一年，比如说1600年，作为开始的一年，并把这一年的3月1日的星期数记作d_{1600}。我们可以去查看古老的纪录来得知它是多少，但这是不必要的，因为它将作为我们的结论的一个推论来得出。

如果没有闰年，那末只要用每过去一年在d_{1600}上加上1的办法，就可得到第N年3月1日的星期数d_N。这样，相应的这个数为

$$d_{1600}+(100C+Y-1600) \pmod 7 . \qquad (8.2.3)$$

考虑到闰年，并假定它们规则地按照每四年一次，那末再应该在这个数上加上

$$\left[\frac{1}{4}(100C+Y-1600)\right]=25C-400+\left[\frac{1}{4}Y\right]. \qquad (8.2.4)$$

这又稍为多了一点，因为世纪年通常不是闰年，所以还应在这个量中减去

$$C-16. \qquad (8.2.5)$$

但当世纪数C可被4整除时，第$100C$年仍是闰年，所以我们

应加上最后一个校正项

$$\left[\frac{1}{4}(C-16)\right]=\left[\frac{1}{4}C\right]-4. \qquad (8.2.6)$$

现在，我们把式(8.2.3)和(8.2.4)相加，减去式(8.2.5)，再加上式(8.2.6)，这就给出了第N年的3月1日的星期数

$$d_N \equiv d_{1600}+124C+Y-1988+\left[\frac{1}{4}C\right]+\left[\frac{1}{4}Y\right] \pmod 7.$$

再按模7简化后，得到

$$d_N \equiv d_{1600}-2C+Y+\left[\frac{1}{4}C\right]+\left[\frac{1}{4}Y\right] \pmod 7. \qquad (8.2.7)$$

让我们把这公式应用于$N=1968$，这一年的3月1日是星期五，因此$d_{1968}=5$。这里

$$C=19, \quad \left[\frac{1}{4}C\right]=4, \quad Y=68, \quad \left[\frac{1}{4}Y\right]=17,$$

我们就得到

$$d_{1968}=5 \equiv d_{1600}+2 \pmod 7.$$

这就给出了$d_{1600}=3$，所以1600年3月1日是星期三。把这代入式（8.2.7），我们就得到了任意一年(第N年）的3月1日的星期数的公式

$$d_N \equiv 3-2C+Y+\left[\frac{1}{4}C\right]+\left[\frac{1}{4}Y\right] \pmod 7. \qquad (8.2.8)$$

其次，我们应当来确定从3月1日到该年的任意其它一天的天数（mod 7）。因为每一个月的天数是变化的，所以为了从数学上来表示这种增加就需要一点技巧。我们先来求出为了得到任意其它月份的第一天的星期数，而需要加到3月1日的星期数上的数目。

因为三月有31天，所以为了得到4月1日的星期数就应加3；因为四月有30天，所以为了得到5月1日的星期数就必须加3+2。这样继续做下去，就可得到下面的加法表。

Ⅰ	三月	0	Ⅶ	九月	16
Ⅱ	四月	3	Ⅷ	十月	18
Ⅲ	五月	5	Ⅸ	十一月	21
Ⅳ	六月	8	Ⅹ	十二月	23
Ⅴ	七月	10	Ⅺ	一月	26
Ⅵ	八月	13	Ⅻ	二月	29

值得指出的是：由于我们以三月一日作为一年的开始，我们实际上已经回到了尤利乌斯·恺撒所实行的古罗马历法，即以九月、十月、十一月、十二月作为第七、第八、第九、第十个月，这正如现在月份的拉丁名字所表示的一样。

让我们回到加法表上来。表中的数虽然是不规则的，但其平均增长数是每月

$$\frac{29}{11}=2.6\cdots.$$

因为第一项是0，所以可以期望第m个月增加的数目应是在$m\cdot 2.6$中减去2.6，并取其整数部分（即$[2.6m-2.6]$，译者注）。但结果发现，这并不完全正确。通过修正被减项，我们得到了正确的表示式

$$[2.6m-2.2]=\left[\frac{1}{5}(13m-11)\right],\qquad m=1,2,\cdots,12. \tag{8.2.9}$$

如果你在式(8.2.9)中核算$m=1,2,\cdots,12$诸值，就会发现我们恰好得到了表中的数值。我们可以骄傲地说，现在一切都好

了！

所以，为了得到第m个月的第一天的星期数，就应该把表示式(8.2.9)加到3月1日的星期数(8.2.8)上去。因为我们所要的是这个月的第d天的星期数，所以应再加上$d-1$。做完这一步，并把所有的项的次序稍加调整，就恰好得到我们所说的公式(8.2.2)。

习　题

1. 求出你的生日的星期数。

2. 当我们仅考虑1900—1999年时，公式(8.2.2)可作怎样的简化？

3. 你所在年级的同学的生日的星期数是怎样分布的？

§8.3　比赛程序表

作为同余理论的另一个简单应用是，安排从象棋到棒球，各种循环比赛的程序表。

我们假定有N个选手或队参加比赛。当N为奇数时，在每一轮比赛中不可能把所有的队都分对进行比赛，而总有一队要轮空。我们可以用这样的办法来克服这一困难：加进一个假想的队T_0，并安排一个包括T_0在内的$N+1$个队的比赛程序表。在每一轮比赛中，被安排和队T_0比赛的队就轮空。所以我们总可以假设有偶数N个队，并给每个队一个编号$x=1, 2, \cdots, N-1, N$。每个队所要进行的比赛的总场数是$N-1$。

现假定x属于集合

$$1,\ 2,\ \cdots,\ N-1. \qquad (8.3.1)$$

在第r轮比赛中，我们指定第x队的对手是第y_r队，y_r属于集合(8.3.1)，并由同余式

$$x+y_r\equiv r \pmod{N-1} \qquad (8.3.2)$$

来确定。为了看出这样的安排将使不同的队有不同的对手，我们只要注意到由

$$x+y_r\equiv r\equiv x'+y_r \pmod{N-1}$$

可推出

$$x\equiv x' \pmod{N-1},$$

由于x，x'同属于集合(8.3.1)，故$x=x'$。

唯一的复杂之处产生于$x=y_r$的情形，这时由式(8.3.2)知必有

$$2x\equiv r \pmod{N-1}。 \qquad (8.3.3)$$

而在式(8.3.1)中，仅有一个x能使这种情形出现。因为若

$$2x\equiv r\equiv 2x' \pmod{N-1},$$

就有

$$2(x-x')\equiv 0 \pmod{N-1}。$$

由于$N-1$是奇数，所以

$$x\equiv x' \pmod{N-1}。$$

因而，式(8.3.3)在集合(8.3.1)中总有一解，即

$$x=\frac{r}{2}, \qquad r\text{ 为偶数},$$

$$x=\frac{r+N-1}{2}, \qquad r\text{ 为奇数}。$$

这样一来，除了满足式(8.3.3)的那个例外的第x_0队外，通过关系式(8.3.2)，对集合(8.3.1)中的每一个队，我们都已指定了它在第r轮比赛中的对手，而我们让第x_0队与第N队进行比赛。

剩下还要指出，通过这样的安排，每一个队在每一轮($r=1,\cdots,N-1$)中都和不同的对手进行比赛。首先，对那

有点儿特殊的第N队来证明这一点．在第 r 轮比赛中，它同由式(8.3.3)确定的第x_0队进行比赛．假定 $s \neq r$，那末在第 s 轮中第N队和第x'_0队比赛，x'_0满足

$$2x'_0 \equiv s \pmod{N-1}.$$

我们不能有$x_0 = x'_0$，因为这将导致

$$2x_0 = 2x'_0 \equiv r \equiv s \pmod{N-1},$$

因而得出 $r = s$。

其次来考虑属于集合(8.3.1)中的第 x 队的各个对手．它和第N队恰好比赛一次，即由

$$2x \equiv r_0 \pmod{N-1}$$

所确定的第 r_0 轮比赛。现假设 $r \neq r_0, s \neq r_0$。这时第 x 队在第 r 轮和第 s 轮的对手将由式(8.3.2)来确定：

$$x + y_r \equiv r \pmod{N-1}, \quad x + y_s \equiv s \pmod{N-1}.$$

和前面一样，$y_r = y_s$ 将再一次导致 $r = s$，所以就证明了 $y_r \neq y_s$。

让我们利用上面所给出的方法，来排一张有$N = 6$个运动员参加的循环赛程序表。经过一些简单的计算就给了由下表列出的结果。在第 r 行第 x 列处的数字表示运动员 x 在第 r 轮比赛中的对手。

r \ x	1	2	3	4	5	6
1	5	4	6	2	1	3
2	6	5	4	3	2	1
3	2	1	5	6	3	4
4	3	6	1	5	4	2
5	4	3	2	1	6	5

习　　题

1. 排出一张有 8 个运动员参加的比赛程序表。

2. 证明，当 $r=2$ 时，第 $1,2,\cdots,N$ 队分别和第 N, $N-1,\cdots,1$ 队进行比赛。

3. 为什么第 $N-1$ 队在第 $r\,(\neq N-1)$ 轮一定是和第 r 队进行比赛？在第 $N-1$ 轮它和哪个队比赛？

4. 若在第 r 轮时，第 x 队和第 y 队比赛，那末，利用公式证明，在这一轮第 y 队也一定是和第 x 队比赛。

§8.4　素数还是合数

作为同余式的最后一个应用，我们将讨论一种检验一个大数是素数还是合数的方法，这是一个十分有效的方法；也是在研究某些随机选取的特殊数时，我们现有的最好的一般方法。这种方法的基础是费马同余式。

设 N 是我们想要检验的数。选取某一与 N 互素的小的数 a。通常合适的是把 a 取为不能整除 N 的小素数，例如 $a=2$，或 $a=3$，或 $a=5$。如果 N 是素数，那末根据费马同余式它应满足

$$a^{N-1}\equiv 1 \pmod{N}. \qquad (8.4.1)$$

因此，如果我们验算这个同余式(8.4.1)，并发现它不成立，那末我们就知道 N 是合数。

例　取 $N=91$，再选 $a=2$。这时

$$a^{N-1}=2^{90}=2^{64}\cdot 2^{16}\cdot 2^{8}\cdot 2^{2}.$$

此外，

$$2^{8}=256\equiv -17 \pmod{91},$$

$$2^{16}=(2^{8})^{2}\equiv(-17)^{2}=289\equiv 16 \pmod{91},$$

$$2^{32}=(2^{16})^2\equiv(\ \ 16)^2=256\equiv-17\pmod{91},$$
$$2^{64}=(2^{32})^2\equiv(-17)^2=289\equiv\ \ 16\pmod{91},$$
所以有
$$2^{90}=2^{64}\cdot2^{16}\cdot2^{8}\cdot2^{2}$$
$$\equiv16\cdot16\cdot(-17)\cdot4\equiv64\not\equiv1\pmod{91}.$$
因此，我们断定N是合数。事实上，$91=7\cdot13$。

我们的例子是太简单了，它不足以表明这个方法的真正威力。利用合适的计算机程序，用这种方法可能去证明某些十分大的数是合数。但遗憾的是，这个方法的缺点是不能指出其因数是什么。因此，在许多例子中，我们可以断定一个数不是素数，但我们对它可能有什么样的因数则一无所知。

特别是这个方法可应用于在§2.3中讨论的费马数
$$F_n=2^{2^n}+1.$$
正如我们指出的，当$n=0,1,2,3,4$时，它们是素数。为了用费马同余式来检验数
$$F_5=2^{2^5}+1=2^{32}+1=4\ 294\ 967\ 297,$$
我们可取$a=3$。若F_5是素数就应该有
$$3^{2^{32}}\equiv1\pmod{F_5}. \qquad (8.4.2)$$
为了计算左边的方幂的余数(mod F_5)，必须取平方32次，并在每一步按模F_5来化简所得结果。这些具体的计算留给读者。我们可以发现同余式(8.4.2)不成立，因此F_5是合数。已知的因数641是通过试除得到的。同样的方法已被用来证明一些更大的费马数不是素数。对其中某些数我们知道它们的因数，而另一些则不知道。

如果同余式(8.4.1)对某个与N互素的a成立，那末N可能是也可能不是素数。对一个合数N，使这一同余式成立的情形是少有的、例外的，所以，通常我们应该猜测N是一

个素数.然而,我们的目的是想要确切地知道它是不是素数。对这个方法加以改进后，这是能够实现的。这一改进是基于这样的事实：**若式(8.4.1)对指数$N-1$成立，但对以$N-1$的任一真除数为指数时就不成立，那末N是素数。**

对不太大的数N还有另一个有效的方法。取$a=2$，波利特和雷麦已经计算出了$N\leqslant 100000000$的在下述意义下的所有例外值：这些N满足

$$2^{N-1}\equiv 1 \pmod N, \qquad (8.4.3)$$

但N是合数。这些数N有时称为**伪素数**。对每一个这种数，他们也给出了最大素因数。

利用波利特的表和雷麦的表，我们可以按照如下的方法来确定任意一个$N\leqslant 100000000$是不是素数：首先检验同余式(8.4.3)是否成立。如果不成立，则N是合数。如果这个同余式成立而N在表中，那末N亦是合数并可从表中得到一个素因数。最后，如果(8.4.3)成立且N不在表中，那末它是素数。

满足同余式(8.4.3)的最小合数是

$$N=341=11\cdot 31.$$

在1000以下还有另外两个，即

$$N=561=3\cdot 11\cdot 17,$$

$$N=645=3\cdot 5\cdot 43.$$

数561是值得注意的，因为当$N=561$时，同余式(8.4.1)对**每一个**与561互素的整数a都成立。我们称这种特别的数有**费马性质**。对于这种数已有很多研究。关于这些数的文献和表可参看D.H.雷麦的《数论表的用法指南》(Guide to Tables in the Theory of Numbers)。

习 题 选 解

§1.3

两题的解答均可见表3（第53页）。

§1.4

1. 假定已知

$$T_{n-1}=\frac{1}{2}(n-1)n.$$

你可以验算这对 $n=2,3,4$ 是成立的。从图1.4.3可以看出 T_n 是由 T_{n-1} 加上 n 而得到的，所以

$$T_n=T_{n-1}+n=\frac{1}{2}n(n+1).$$

2. 从图1.4.4可看出：为了得到 P_n 必须在 P_{n-1} 上加上

$$1+3(n-1)=3n-2.$$

如果我们已经知道

$$P_{n-1}=\frac{1}{2}(3(n-1)^2-(n-1))$$

（根据表(1.4.3)知，这对 $n=2,3,4$ 是成立的），那末就推出：

$$P_n=P_{n-1}+3n-2=\frac{1}{2}(3n^2-n).$$

3. 第 n 个 k 角数是由第 $(n-1)$ 个再加上

$$(k-2)(n-1)+1$$

而得到的，我们可以用解问题 2 的同样的方法导出所要的公式。问题 2 和 3 可以有不同的解法：把这些点分为如图1.4.4所示的三角形，并利用关于T_n的公式。详细写出这样的证明。

§1.5

1．例如下面也是这样的幻方：

16	3	2	13
9	6	7	12
5	10	11	8
4	15	14	1

这是由交换度勒幻方中的第二行和第三行而得的。另一个不那么显然的是

16	4	1	13
9	5	8	12
6	10	11	7
3	15	14	2

2．因为在 4 × 4 的幻方中的数不能超过16，所以仅有两个年份是可能的，即1515和1516。第一个显然除外，而对第二个可以发现不可能作出这样一个幻方。

§2.1

2．1979。

3．从114到126这些数均为合数。

§ 2.3

1. $n=3, 5, 15, 17, 51, 85$.
2. 我们有

$$\frac{360^\circ}{51}=6\cdot\frac{360^\circ}{17}-\frac{360^\circ}{3}.$$

3. 由第一到第五个费马素数所给出的这种乘积（使对应的正多边形可以作出）总共有

$$5+10+10+5+1=31$$

个不同的数。最大值是

$$n=3\cdot5\cdot17\cdot257\cdot65537=4\ 294\ 967\ 295.$$

§ 2.4

1. 以一百个数为一组，在开头的十组中的素数个数依次为
   24，20，16，16，17，14，16，14，15，14。
2. 有11个这样的素数。

§ 3.1

1. $120=2^3\cdot3\cdot5$；　$365=5\cdot73$；　$1970=2\cdot5\cdot197$.
3. $360=2\cdot2\cdot90=2\cdot6\cdot30=2\cdot10\cdot18=6\cdot6\cdot10$.
4. 一个数是偶素数仅当它形为$2k$，k是奇数。假定一个数n有偶素数分解式

$$n=(2k_1)\cdot(2k_2)\cdot\cdots,$$

这里至少有两个因数。这可导出另一个这样的分解式

$$n=(2k_1\cdot k_2)\cdot2\cdot\cdots.$$

除了当$k_2=1$外，这和第一个是不同的。同样的理由可应用于下面的$k_3,k_4,\cdots$。这样，我们证明了若有唯一的

偶素数分解式，那末一定要

$$n=(2k)\cdot 2\cdot 2\cdot\cdots=k\cdot 2^{a},\quad k\text{奇数。}$$

容易看出，当 $k=1$，即 $n=2^{a}$时，这是唯一的分解式。若 $k>1$，那末还要有进一步的条件：k 必须是一个通常的素数。因为，如果 $k=a\cdot b$，那末就有另一个分解式，即

$$n=(2a)\cdot(2b)\cdot 2\cdot 2\cdot\cdots.$$

§3.2

1. 素数有两个除数；素数幂 p^{a} 有 $a+1$ 个除数。
2. $\tau(60)=12$，　$\tau(366)=8$，　$\tau(1970)=8$。
3. 对于不超过 100 的数，除数个数最多是12个，并由下列各数

   72，84，90，96

   达到。

§3.3

1. 24，48，60，10080。
2. 2^{13}，180，45360。
3. 24和36。
4. 设除数个数为 $r\cdot s$，r 与 s 是素数。那末

   $$n=p^{rs-1}\quad\text{或}\quad n=p^{r-1}\cdot q^{s-1},$$

   p,q 是素数。

§3.4

1. 8128和33550336。

§ 4.1

1. (a) $(360,1970)=10$; (b) $(30,365)=5$.
2. 假定$\sqrt{2}$是有理数

$$\sqrt{2}=\frac{a}{b}.$$

相约之后可假定 a 与 b 沒有公因数。平方后得到

$$2b^2=a^2.$$

由于唯一分解定理，a 可被 2 整除，因此 a^2 可被 4 整除。再根据 b^2 的素因数分解式的唯一性，所以 b 也可被 2 整除，而这与 a 和 b 沒有公因数的假定相矛盾。这一矛盾指出我们原来的$\sqrt{2}$的有理表达式是不存在的。

§ 4.2

1. 奇数。
2. 若 p 是任一个可以整除 n 与 $n+1$ 的素数，那末它也应该整除 $(n+1)-n=1$。
3. 沒有一对数是互素的。
4. 成立。

§ 4.3

2. $(220,284)=4$, $(1184,1210)=2$,
$(2620,2924)=4$, $(5020,5564)=4$.
3. 为了确定能够整除

$$n!=1\cdot2\cdot3\cdot\cdots\cdot n$$

的10的最高次幂，我们首先要求出整除它的 5 的最高次幂。每第五个数可被 5 整除：

$$5,\ 10,\ 15,\ 20,\ 25,\ 30,\ \cdots,$$

不超过 n 的这些数总共有 $\left[\frac{n}{5}\right]$ 个。但其中有一些可被 5 的二次幂整除，即是25,50,75,100,…，而这一些总共有 $\left[\frac{n}{25}\right]$ 个。那些也可被三次幂 $125=5^3$ 整除的数是125，250,275,…，它们共有 $\left[\frac{n}{125}\right]$ 个，等等。这就证明了可以整除 $n!$ 的 5 的最高次幂的指数是

$$\left[\frac{n}{5}\right]+\left[\frac{n}{5^2}\right]+\left[\frac{n}{5^3}\right]+\cdots, \tag{E}$$

这里，这些项一直加到分母超过分子时为止。

完全同样的论证可用于求任一其它的素数的最高次幂，特别地，当 $p=2$ 时可求得指数为

$$\left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\left[\frac{n}{2^3}\right]+\cdots.$$

显然，这个指数不小于表示式(E)中的指数，所以 $n!$ 中每一个因数 5 必能和一个因数 2 相结合。这样一来，(E) 也给出了整除 $n!$ 的10的最高次幂，亦即这个数末尾的零的个数。

例 $n=10$，$\left[\frac{10}{5}\right]=2$，$\left[\frac{10}{5^2}\right]=0$，所以 $10!$ 以两个零结尾。

$n=31$，$\left[\frac{31}{5}\right]=6$，$\left[\frac{31}{5^2}\right]=1$，$\left[\frac{31}{5^3}\right]=0$，所以$31!$ 以 7 个零结尾。

§4.4

1. $[360,1970]=70920$，$[30,365]=2190$.

2. $[220,284]=15620$，$[1184,1210]=716320$，
$[2620,2924]=1915220$，$[5020,5564]=6982820$.

§5.2

1. $m=8$，$n=1$，$(16,63,65)$，$n=3$，$(24,55,73)$，
$n=5$，$(80,39,89)$，$n=7$，$(112,15,113)$；
$m=9$，$n=2$，$(36,77,85)$，$n=4$，$(64,65,97)$，
$n=8$，$(144,17,145)$；
$m=10$，$n=1$，$(20,99,101)$，$n=3$，$(60,91,109)$，
$n=7$，$(140,51,149)$，$n=9$，$(180,19,181)$.

2. 不能。如果
$2mn=2m_1n_1$，$m^2-n^2={m_1}^2-{n_1}^2$，$m^2+n^2={m_1}^2+{n_1}^2$，
就将推出
$$m^2=m_1^2,\ n^2=n_1^2 \quad 或 \quad m=m_1,\ n=n_1.$$

3. 当数 c 是一个毕达哥拉斯三角形的斜边时，c 的每一个倍数kc 也有同样的性质。这样一来，我们只需要去列出那些不超过100的值 c，这些 c 没有一个除数可以作为斜边。从上面所列出的本原解中我们可以求得这些值是
$$c=5,13,17,29,37,41,53,61,73,89,97.$$

§5.3

1. $(120,50,130)$，$(624,50,626)$，$(48,14,50)$，
$(40,30,50)$，$(120,22,122)$.

2. $100=10^2+0^2$，$101=10^2+1^2$，$104=10^2+2^2$，

$106=9^2+5^2$,　　$109=10^2+3^2$.

数101,106,109是本原毕达哥拉斯三角形的斜边。

3. 没有面积为78或1000的毕达哥拉斯三角形。有一个面积为120的三角形(24,10,26)。

4. 这些数不是任一毕达哥拉斯三角形的周长。

§6.2

1. 194和364。

2.
$$362=(1,0,1,1,0,1,0,1,0)_2$$
$$=(1,4,0,2)_6=(1,4,5)_{17},$$
$$1969=(1,1,1,1,0,1,1,0,0,0,1)_2$$
$$=(2,2,0,0,2,2,1)_3=(6,13,14)_{17},$$
$$10000=(1,0,0,1,1,1,0,0,0,1,0,0,0,0)_2$$
$$=(1,1,1,2,0,1,1,0,1)_3=(2,0,10,4)_{17}.$$

§6.3

1. 数 $2,3,\cdots,b-1$ 中的每一对数的乘积都是非显然乘法。因为乘法的次序是不重要的，所以我们可先考虑最小的因数。这样，有 $b-2$ 个包含因数 2 的乘积，即
$$2\cdot2,\ 2\cdot3,\ \cdots,\ 2\cdot(b-1);$$
有 $b-3$ 个以 3 为最小因数的乘积，即
$$3\cdot3,\ 3\cdot4,\ \cdots,\ 3\cdot(b-1).$$
继续这样做下去可以看出有
$$(b-2)+(b-3)+\cdots+3+2+1$$
$$=\frac{1}{2}(b-1)(b-2)$$
个非显然乘积。

2. 如果我们在这些乘积中包括有因数 1 的乘积，那末通过展开

$$[1+2+\cdots+(b-1)][1+2+\cdots+(b-1)]$$

可得到所有这些乘积，而这等于

$$\left[\frac{1}{2}b(b-1)\right]^2.$$

对 $b=10$ 这给出 $45^2=2025$。若因数 1 除外，则和为

$$[2+\cdots+(b-1)][2+\cdots+(b-1)]$$
$$=\left[\frac{1}{2}(b+1)(b-2)\right]^2.$$

对 $b=10$ 可求出和为 $(44)^2=1936$。在这两个情形中，和均是一个平方数。

§6.4

1. 函数

$$f(b)=\frac{b}{\log b}$$

在区间 $1<b<\infty$ 内是正的，且当 $b\to1$ 或 $b\to\infty$ 时，$f(b)\to\infty$。其导数

$$f'(b)=\frac{\log b-\log e}{(\log b)^2}$$

仅当

$$b=e=2.71828\cdots$$

时为零，而在区间 $1<b<e$ 内，它为负，所以 $f(b)$ 为递减；在区间 $e<b<\infty$ 内，它为正，所以 $f(b)$ 为递增。因而最小值为

$$f(e)=\frac{e}{\log e}=6.25907\cdots.$$

当 $1<b<\infty$ 时，函数

$$g(b)=\frac{b-1}{\log b}$$

是正的，且 $g(b)\to\frac{1}{\log e}$；当 $b\to 1$ 时，$g(b)\to\infty$，当 $b\to\infty$ 时，其导数为

$$g'(b)=\frac{\log b-\left(1-\frac{1}{b}\right)\log e}{(\log b)^2}.$$

由于上式右边分子的导数为

$$\left(1-\frac{1}{b}\right)\frac{\log e}{b}>0,\quad 1<b<\infty,$$

所以在区间 $1<b<\infty$ 内，$g'(b)$ 是正的，故而函数 $g(b)$ 是递增的①。

§6.5

1. $2^n+1=(1,0,0,\cdots,0,1)_2$，其中有 $n-1$ 个零。
2. $2^p-1=(1,1,\cdots,1)_2$，其中有 p 个1，因而

$$2^{p-1}(2^p-1)=(1,\cdots,1,0,0,\cdots,0)_2$$

其中有 p 个1及 $p-1$ 个零。

§6.6

2.
```
 411
 411
 411
 714
----
1947
```

4.
```
29786
  850
  850
-----
31486
```

5.
```
 92836
 12836
------
105672
```

① 这一题的解答原书有误，因为这里的对数是以10为底的。——译者

问题 1 和 3 留给你自己去做。如果你有困难的话，可同懂计算机的人商量。

§7.2

1. $-37\equiv 5 \pmod 7$， $-111\equiv 10 \pmod{11}$，
   $365\equiv 25 \pmod{30}$。

§8.2

1. 对 $C=19$，公式（8.2.2）中的最后两项可化简为

$$\left[\frac{1}{4}C\right]-2C\equiv 1 \pmod 7.$$

§8.3

1.

1	2	3	4	5	6	7	8
7	6	5	8	3	2	1	4
8	7	6	5	4	3	2	1
2	1	7	6	8	4	3	5
3	8	1	7	6	5	4	2
4	3	2	1	7	8	5	6
5	4	8	2	1	7	6	3
6	5	4	3	2	1	8	7

2. 当 $r=2$时，例外情形出现于 $x=1$。因此，第 1 队和第8队比赛及第 8 队和第 1 队比赛；对其它的值$x=2,3,\cdots,7$，我们有

$$y\equiv 2-x\equiv 9-x \pmod 7,$$

所以对应地有 $y=7,6,\cdots,2$。

3. 在第 r 轮比赛中，第 $N-1$ 队和第 y 队比赛；

$$y \equiv r-(N-1) \equiv r \pmod{N-1}.$$

仅当

$$2(N-1) \equiv r \pmod{N-1}$$

时，第 $N-1$ 队才可能是例外的，而这时必有 $r=N-1$，在这一轮中第 $N-1$ 队和第 N 队比赛。

4． 当 x 不是例外情形时，条件（8.3.2）对 x 和 y_r 是对称的。当 x 满足式（8.3.3）时，它和第 N 队比赛，而根据定义第 N 队和第 x 队比赛。

参考书目①

[1] O.Ore, Number Theory and Its History.

[2] B.W.Jones, The Theory of Numbers.

[3] W.J.LeVeque, Elementary Theory of Numbers.

[4] C.T.Long, Elementary Introduction to Number Theory.

[5] N.H.McCoy, The Theory of Numbers.

[6] I.Niven and H.S.Zuckerman, Introduction to the Theory of Numbers.

[7] H. Rademacher, Lectures on Elementary Number Theory.

[8] 维诺格拉陀夫，数论基础，商务印书馆，1952。

[9] H.Cohn, A Second Course in Number Theory.

[10] E.Grosswald, Topics from the Theory of Numbers.

[11] G.H.Hardy and E.M. Wright, An Introduction to the Theory of Numbers.

[12] W.J.LeVeque, Topics in Number Theory (2 vols).

[13] D.Shanks, Solved and Unsolved Problems in Number Theory.

[14] L.E.Dickson, History of the Theory of Numbers (3 vols).

[15] D.H.Lehmer, Guide to Tables in the Theory of Numbers.

[16] 华罗庚，数论导引，科学出版社，1979。

[17] 闵嗣鹤，严士健，初等数论，人民教育出版社，1982。

[18] 柯召，孙琦，初等数论100例，上海教育出版社，1980.

[19] 柯召，孙琦，谈谈不定方程，上海教育出版社，1980.

[20] 陈景润，初等数论，Ⅰ，Ⅱ，科学出版社，1978，1980。

[21] 王元，谈谈素数，上海教育出版社，1978。

[22] 潘承洞，素数分布与哥德巴赫猜想，山东科学技术出版社，1979。

---

① 为了进一步学习的方便，我们补充了参考书[16]—[22]。——译者